

# Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security





Powering the digital economy:  
Regulatory approaches to  
securing consumer privacy,  
trust and security

The report was prepared by ITU experts; Laurits Ketscher and Jason Harle from Deloitte Denmark, under the direction of the ITU/BDT Regulatory and Market Environment Division, in collaboration with the ITU/BDT ICT applications & Cybersecurity Division and the Asia and Pacific Regional Office, and in close coordination with the Chief of the ITU/BDT Infrastructure, Enabling Environment, and E-Applications Department. The ITU team included Kemal Huseinovic, Sofie Maddens, Nancy Sundberg, Sameer Sharma, Marco Obiso and Hani Eskandar. The report was edited by Piers Letcher.

### ISBN

978-92-61-28141-0 (Paper version)  
978-92-61-28151-9 (Electronic version)  
978-92-61-28161-8 (ePub version)  
978-92-61-28171-7 (Mobi version)

The views expressed in this report are those of the authors and do not necessarily reflect the opinions of ITU or its Membership.



© International Telecommunication Union, 2018

Some rights reserved. This work is available under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO licence (CC BY-NC-SA 3.0 IGO; <https://creativecommons.org/licenses/by-nc-sa/3.0/igo>).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited, as indicated below. In any use of this work, there should be no suggestion that ITU endorses any specific organization, products or services. The unauthorized use of ITU names or logos is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: “This translation was not created by the International Telecommunication Union (ITU). ITU is not responsible for the content or accuracy of this translation. The original English edition can be found at: [www.itu.int/treg](http://www.itu.int/treg)”.

**Suggested citation.** Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security, International Telecommunication Union, 2018. Licence: CC BY-NC-SA 3.0 IGO.

# Table of Contents

Foreword	v
Executive Summary	vi
1. Introduction	1
2. Exploring online privacy, trust and ensuring security: setting the scene (global and regional)	4
2.1 The threat and power of the digital economy	4
2.2 Declining trust in the digital economy	6
2.3 Empowering the app economy	8
2.4 Digital identities	9
2.5 Legislative approaches to privacy and competition	10
2.6 The right to be anonymous?	11
3. Understanding online data business models and data markets	12
3.1 Data and the two-sided marketplace	12
3.2 How do these apps make their money?	13
3.3 Who controls your data?	14
3.4 Data ownership, privacy and competition considerations	15
3.5 What are the pressure points?	17
3.6 Openness and trust	18
4. Models of ensuring protection, privacy and trust	19
4.1 Understanding EU GDPR	21
4.2 What does EU GDPR mean for citizens?	22
4.3 Different models for data protection regulation	23
4.4 Adoption of guidelines	27
4.5 Implications of EU GDPR on other regions, with a special view to Asia	28
4.6 Data localization, national security and cross border restrictions	30
4.7 EU-GDPR – the new <i>de facto</i> global regulation?	31
5. A focus on digital identity within the framework protection of personal data	32
5.1 Digital identity	32
5.2 Basic security	33
5.3 Privacy considerations	34
5.4 Digital identity examples	34
5.5 Dynamic digital identities and cross-sectoral regulation	35
6. Data security	36
6.1 What barriers does industry face in securing data?	37
6.2 Regulators	38
6.3 Manufacturers	39
6.4 Distributed ownership, distributed risk	41
7. Conclusion	42

# List of Tables, Figures and Boxes

## Tables

Table 1 – Roles of digital personal data actors	3
Table 2 – Mobile phone feature usage in passive and active data collection.	13
Table 3 – Building trust across cultures	18
Table 4 – Core Data Protection Principles (UNCTAD)	21
Table 5 – Regulatory design options	24
Table 6 – Regulatory design options table, with examples	27

## Figures

Figure 1 – Examples of personal data	2
Figure 2 – The circle of mistrust (Wernberg 2007)	7
Figure 3 – App economy value chain (with privacy and security considerations)	9
Figure 4 – Collaboration between ICT regulators and Data Protection Authorities	16
Figure 5 – National data protection and privacy by region (ITU) and worldwide (UNCTAD)	20
Figure 7 – Types of restrictions on cross-border data flows	29
Figure 8 – Blockchain	40

## Boxes

Box 1: Artificial Intelligence (AI) and privacy	5
---	---

I am pleased to present this report on *Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security* prepared by the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU).

The networked digital environment offers extraordinary and unprecedented potential for social and economic growth. It offers boundless opportunities for governments to create efficiencies and improve the lives of their citizens. And it offers businesses, large and small, new and better ways to connect with their users and consumers around the world.

In this new era of the digital economy, data has become one of the world's most valuable commodities as it is neither finite nor physical, and can be easily transmitted and duplicated.

One of the key issues that need to be addressed is how to encourage the growth of the digital economy, powering and driving it forward, while still offering consumers the protection and privacy they require, and creating an atmosphere of trust in the online world. Consumer data protection, trust and security are perhaps some of the greatest remaining challenges to an ever-expanding digital economy. This is all the more important in a world seeing reports of increased data breaches and compromised personal data.

This report explores the issues of online privacy, trust and security, and how these influence and drive online data business models and data markets, in the light of data ownership, privacy and competition considerations. It looks at the nature of personal data, and how attitudes to it are shifting, particularly as social media and the online spheres evolve.

The report goes on to look at examples of data protection regulation, and in particular the European Union's General Data Protection Regulation, which came into force in May 2018. It also examines other different models for data protection along with their specific advantages and disadvantages.

Underpinning all of these efforts in terms of powering the digital economy is the notion of trusted digital identity, and the report goes on to explore some of the issues concerned, including data security, and the impact this has on industry, regulators and manufacturers, concluding with a look at the potential implications of new technologies such as blockchain.

This report clearly shows that there is tremendous potential for growth and prosperity in the new digital ecosystem – but every effort must be put in place to make sure that data protection, security and trust issues are properly addressed as we move forward. It is my hope that this report will make a timely and important contribution to this discussion.



Brahima SANOU  
Director, Telecommunication Development Bureau

# Executive Summary



This report deals with the question of how to guarantee trust and privacy in order to power the digital economy. Although the world continues to embrace digitalization and digital solutions, trust in these solutions is decreasing, potentially limiting or even damaging the promise of the global digital economy. The report provides an outline of the value and the functioning of the digital economy, as well as requirements and considerations in terms of ICT and privacy regulation. It argues that in order to ensure continued and sustained growth, there needs to be more focus on privacy and security. In order to achieve the full potential, private actors, governments and regulators will need to work together to address the many challenges faced in creating an environment of trust and confidence in the digital economy.

## **Key messages**

The *report* helps leaders, policy makers and regulators identify the main aspects that need to be addressed in terms of securing consumer privacy, trust and security.

- The report emphasizes the **growing importance of the digital economy**, with more than 4.2 billion active mobile broadband subscriptions worldwide at the end of 2017, and more than 3.5 billion users online. Technology is there, and customers, attracted by lower service prices and convenience, are there. But consumer privacy, trust and security still remain major barriers to an ever-expanding digital economy.
- The report sets the scene by looking at the **threat and power of the digital economy** and declining trust, with numerous high-profile data breaches and compromises to personal data. It contrasts that with the growing importance of the app economy, which is forecast to be worth USD 6.3 trillion annually by 2021, and legislative approaches to privacy and competition.
- The report looks at the **growing importance of data** – which is so important that it is now one of the world’s most valuable commodities, and has been described as ‘the new oil’. It goes on to examine issues of data ownership and control.



- One of the most important pieces of regulation to be enacted in this area is the **European Union’s General Data Protection Regulation (GDPR)**, which came into force in May 2018, and the report looks at what it means for different actors, and its implications on other regions. It also looks at different models for data protection regulation, and notes that different models will be needed in different circumstances.
- Online privacy and trust, and data protection depend to a considerable extent on **digital identity**, and the report provides analysis of what this means in terms of security as well as providing a number of examples of countries which have rolled out national digital identity programs, including Denmark, Estonia and India.
- Finally, the report looks at the important issue of **data security**, and potential barriers faced in implementing solutions – and notes the potential importance of blockchain technology in providing better data security moving forward.





Figure 1 – Examples of personal data



Source: European Commission.

According to article 9 of the European Union's General Data Protection Regulation (EU GDPR)<sup>3</sup>, special (sensitive) categories of personal data include, among others: health data, genetic data, biometrics, religious beliefs and political beliefs. Stricter rules apply to processing and handling of these special data, and such data enjoy greater protection than ordinary personal data (article 6<sup>4</sup>) which encompasses all personal data not listed in article 9.

Under most of the different global data protection regimes, private companies may collect personal data, but they do not 'own' the data. Instead, they 'control' the data, and are therefore legally referred to as 'data controllers', while the data itself remains the property of the individual. This applies to both the European and APEC/ASEAN models, which build on the OECD guidelines first providing these definitions in the 1980s (see chapter 4).

Two major events from the first half of 2018 are having a significant impact on the way organizations and individuals are viewing and managing their relationships with personal data.

On 17 March, both the Guardian and New York Times published articles concerning a London-based company, Cambridge Analytica, that had reportedly harvested 50 million Facebook profiles (later revised to 87 million). The company was accused of seeking to use aggregated data to affect the outcome of major political events in 2016, including the UK referendum on its membership of the European Union, and the United States presidential election, using personalized political advertisements<sup>5</sup>.

On 25 May, just two months later, EU GDPR came into force. At a time when data protection was making significant media headlines, GDPR delivered explicit criteria and rules on who was affected,

<sup>3</sup> <https://gdpr-info.eu/art-9-gdpr/>

<sup>4</sup> <https://gdpr-info.eu/art-6-gdpr/>

<sup>5</sup> <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Accessed 22 October 2018

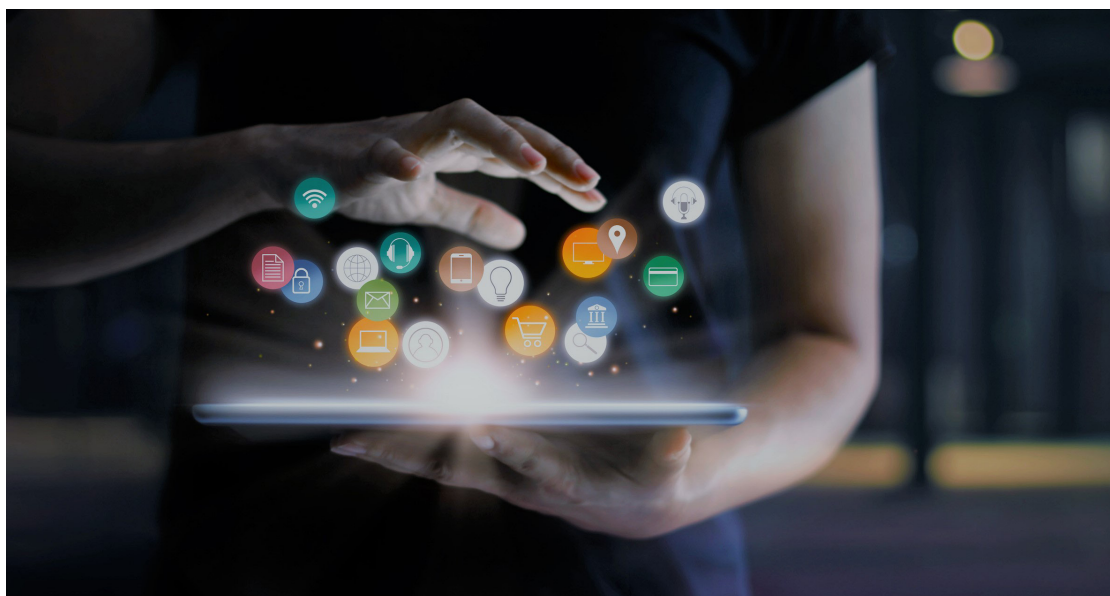
Table 1 – Roles of digital personal data actors

Governments	<ul style="list-style-type: none"> <li>• Adopt the necessary national legislation to ensure proper data protection</li> <li>• Choose between different legal models for data protection (see chapter 4)</li> <li>• Set the overall rules for the collection, transfer and retention of personal data</li> <li>• Ensure that data protection is prioritized with the necessary funding and enforcement.</li> </ul>
Regulators	<ul style="list-style-type: none"> <li>• Regulate data protection across different industries and sectors</li> <li>• Cooperate across regulatory areas with data protection authorities, consumer protection agencies, competition authorities, antitrust bodies and ICT/Telecom regulators</li> <li>• Raise awareness about data protection, privacy and security rules and regulations in place.</li> <li>• Inform consumers of their rights</li> <li>• Aid the private sector in regulatory efforts, either through co-regulation or facilitating compliant self-regulation</li> <li>• Conduct privacy impact assessments when developing rules and regulations</li> <li>• Facilitate the creation and adoption of industry and sector specific standards for data protection</li> <li>• Enforce and uphold individual data protection rights.</li> </ul>
Private sector	<ul style="list-style-type: none"> <li>• Understand and act according to applicable data protection laws</li> <li>• Ensure the transparent and lawful processing of personal data</li> <li>• Define and enforce internal guidelines, procedures and governance structures for handling personal data</li> <li>• Conduct privacy assessments on high-risk activities</li> <li>• Contribute to the creation and adoption of sector specific standards for data protection and privacy</li> <li>• Ensure the enforcement and upholding of individual data protection rights in their activities.</li> </ul>
Consumers	<ul style="list-style-type: none"> <li>• Be aware of the data they give away, and the services they receive in return</li> <li>• Actively engage in and understand public data protection debates</li> <li>• Hold data controllers accountable.</li> </ul>

what could and could not be done with personal data, and enforcement action for those organizations that did not adhere to the regulations. Crucially, the reach of GDPR is not limited to people inside the EU, but also covers companies controlling or processing personal data of EU citizens in any country, effectively making it a quasi-global set of regulations.

The digital economy is vital to continued global growth, but it also comes with risks and traps, which threaten to dampen global growth rates, as consumer trust is eroded, while new privacy laws push companies and regulators to put privacy and security to the fore, and change their ways of doing business.

Consumer trust and legal compliance need to be front and centre in powering the digital economy and driving digital development. Companies must consider privacy and cybersecurity as integrated parts of their services, and at the forefront of future development and innovations across the entire ICT industry. Regulators, for their part, need to understand the digital economy, technological advances, and the challenges facing both consumers and companies.



## 2. Exploring online privacy, trust and ensuring security: setting the scene (global and regional)

### 2.1 The threat and power of the digital economy

There is no doubt that the Internet – and the free flow of data it has enabled – has been a significant driver of the global digital economy. In the digital landscape, the free flow of data beyond borders has proven to be a force of economic growth and globalization, and global data flows were estimated to have delivered an extra 3.5% to global GDP in 2014<sup>1</sup>.

Advances in technology, such as cloud solutions, have made it easy and convenient for businesses to get access to applications and technology on-demand or pay-per-use, rather than tying up scarce liquidity in complex investments. Today, you only need a laptop with Internet access to create an online business and begin marketing your goods or services to consumers and companies all over the world. This has dramatically reduced the cost of entry to the business world, especially for small and medium enterprises (SMEs).

Advances in cloud technology have also made it possible for businesses to start up in otherwise difficult data-heavy areas of business, such as banking and insurance, which are now seeing growth in competition from online providers with no physical branches<sup>2</sup>.

At the same time, international trading platforms, such as Alibaba and Amazon, help drive sales for Asia- and Pacific-based SMEs. Through these platforms, they can reach a global audience, while the platforms themselves offer additional services, such as handling shipping and customer management.

Underlying this massive growth is the flow of data. Data is the new currency for businesses (see chapter 3 for a more in-depth discussion), and a significant subset of this is personal data. Personal data is a primary fuel for the digital revolution, and the direct marketing and selling of goods and services

<sup>1</sup> [https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy\\_meltzer\\_lovelock\\_web.pdf](https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf) Accessed 22 October 2018

<sup>2</sup> <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-maintaining-control-in-the-cloud.pdf> Accessed 22 October 2018

to individuals. Services such as Google derive significant parts of their revenue from the profiling and use of the personal data they collect, allowing them to target their users directly with various products and services. Services such as E-bay, Alibaba and Amazon, meanwhile, provide platforms that provide the option both to exploit data as well as to collect it.

Targeted advertising means that people all over the world receive advertisements based on their online activity and personal interests, making it more likely for them to buy consumer goods and services. Data is increasingly used to profile users based on, among other things, their online search history, active social media commentary, tagged geo-locations and online purchases, and including confidential and personal information regarding their political preferences, sexual orientation, and much more. While targeted advertising can seem harmless, it is important to recognize that it is based on a system designed to harvest personal data, and which distributes this data widely across borders, sometimes in unintended ways.

Even though companies may wish to treat personal data with a respect for privacy, they may well end up inadvertently violating the privacy of their users by using cookies and tracking programs to monetize on the traffic flow, and also inadvertently share this data with third parties, losing control over who receives and uses their own visitors' data.

### Box 1: Artificial Intelligence (AI) and privacy

Many of today's most significant AI systems are made possible through the acquisition and analysis of large corpora of (potentially personal) data. And the range and depth of personal data acquired by AI systems are on the rise. For example, voice-driven conversational assistants, such as Alexa (Echo), Siri, and Cortana, may be more likely to know detailed private information such as what you are eating. What is clear is that users, and policymakers, are increasingly sensitive to privacy issues that arise from artificial intelligence.

Privacy concerns, made manifest when AI is applied to social media profile data, has a lot in common with the privacy issues that impact telecommunications operators. While at first blush it may seem that mobile operators hold relatively basic digital records of their users, such as cell tower derived user position data, a relatively small amount of mobile location data can be used to identify individuals uniquely. In this way, even anonymized data can be relatively easily de-anonymized. Researchers have shown that 'the uniqueness of human mobility traces is high, thereby emphasizing the importance of the idiosyncrasy of human movements for individual privacy. Indeed, this uniqueness means that little outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale, and coarse mobility dataset,' (de Montjoye, Hidalgo, Verleysen, & Blondel, 2013). In turn, this locational data can be used to infer private details of the individual (Blumberg & Eckersley, 2009).

Thus the data privacy concerns that arise out of AI systems (including those based on social media profile data analysis) have significant similarities to the data privacy concerns already present with telecommunication user data (including mobile location data). Both data sets, when subject to powerful analysis, can turn even public and seemingly benign information into deeply personal detail. This challenge will grow even for operator held user data sets as the capabilities of AI-driven analytics expands. AI engines, applied to an operator's user data, may result in intimate private user information almost at the scale held by social media platforms.

Source: Artificial Intelligence (AI) for Development Series, Module/Chapter on AI ethics and society, ITU, 2018.

Other parties may seek to deceive the data controller, and deceitfully give away data to third parties, who may misuse the data without the knowledge of the data controller. Such was the case with

Cambridge Analytica, who used the personal data of more than 87 million Facebook users to create targeted political advertisements aimed at influencing the results of political events in 2016, as discussed earlier. The targeted advertisements, created through political profiling, played on the fears and prejudices of specific groups, encouraging opposition voters to abstain from voting, or to vote for a third party candidate.

Last but not least, there is the increase in cyberattacks, which often affect the personal data held by companies or public authorities. In June 2018, Singapore, according to the Minister of Health, was hit by a state-sponsored attack that resulted in losing 1.5 million citizens' digital health and identity data, including the Prime Minister's<sup>3</sup>. The success of these attacks helps to corrode public and consumer trust in the different entities responsible for handling personal data.

Cyberattacks are increasing in terms of both scale and volume, across the public and private sectors<sup>4</sup>. Global ransomware attacks, such as WannaCry and Petya/NotPetya, hit public authorities and private companies on a global scale, by holding their data encrypted, in exchange for a ransom. Meanwhile crypto-jacking exploits vulnerabilities in Internet of Things (IoT) devices, to make the devices mine cryptocurrencies for the attackers, without the owners' knowledge<sup>5</sup>. On average it takes a company 146 days to detect a cyberattack, by which time their customers' or clients' personal data or their business sensitive data may be irreversibly compromised<sup>6</sup>. It is estimated that global damages caused by cyberattacks will exceed USD 6.3 trillion by 2021, up from USD 3.1 trillion in 2017<sup>7</sup>.

## 2.2 Declining trust in the digital economy

Consumers have little or no influence over their personal data online, and this, coupled with increasing numbers of cyberattacks, has led to a loss of trust in online service providers. A 2017 Gigya survey of more than 4,000 UK and American consumers found that more than 68% do not trust brands to handle their personal information<sup>8</sup>. A similar study conducted by the Information Commissioner's Office (ICO) in the UK in 2017 found that a majority of the UK public does not trust organizations with their data, partly due to security concerns and partly due to the lack of transparency and control over their personal data<sup>9</sup>.

Similarly, the 2018 *CIGI-Ipsos Global Survey on Internet Security and Trust*, conducted by the United Nations Conference on Trade and Development (UNCTAD), and covering more than 25,000 Internet users across 25 countries, concluded that more than half of respondents are more concerned about their online privacy than they were one year ago, and that 81% attributed this to increased concern about cybercriminals<sup>10</sup>. The UNCTAD study found different levels of trust between Internet users in emerging and mature markets. Emerging economies have the largest proportion of Internet users who claim that they have trust in the Internet, with 91% in China; 90% in India; 88% in Indonesia; 87% in Pakistan; and 84% in Mexico. Trust in the Internet in Japan and Tunisia, by contrast, was expressed by under 60% of users. Fen Osler Hampson, CIGI's director of global security and politics, suggests that 'newcomers to the Internet might be unaware of potential abuses and risks. Yet, this trust is essential for the successful expansion and use of e-commerce platforms and mobile payment systems

<sup>3</sup> <https://www.bbc.com/news/world-asia-44900507> Accessed 19 October 2018

<sup>4</sup> <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf> Accessed 21 October 2018

<sup>5</sup> <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf> Accessed 21 October 2018

<sup>6</sup> [http://download.microsoft.com/download/C/F/6/CF62335F-C46B-4D84-B0C9-363A89B0C5E6/Microsoft\\_advanced\\_threat\\_analytics\\_datashet.pdf](http://download.microsoft.com/download/C/F/6/CF62335F-C46B-4D84-B0C9-363A89B0C5E6/Microsoft_advanced_threat_analytics_datashet.pdf) Accessed 21 October 2018

<sup>7</sup> <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf> Accessed 21 October 2018

<sup>8</sup> <https://www.gigya.com/resource/report/2017-state-of-consumer-privacy-trust/> Accessed 21 October 2018

<sup>9</sup> <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/11/ico-survey-shows-most-uk-citizens-don-t-trust-organisations-with-their-data/> Accessed 21 October 2018

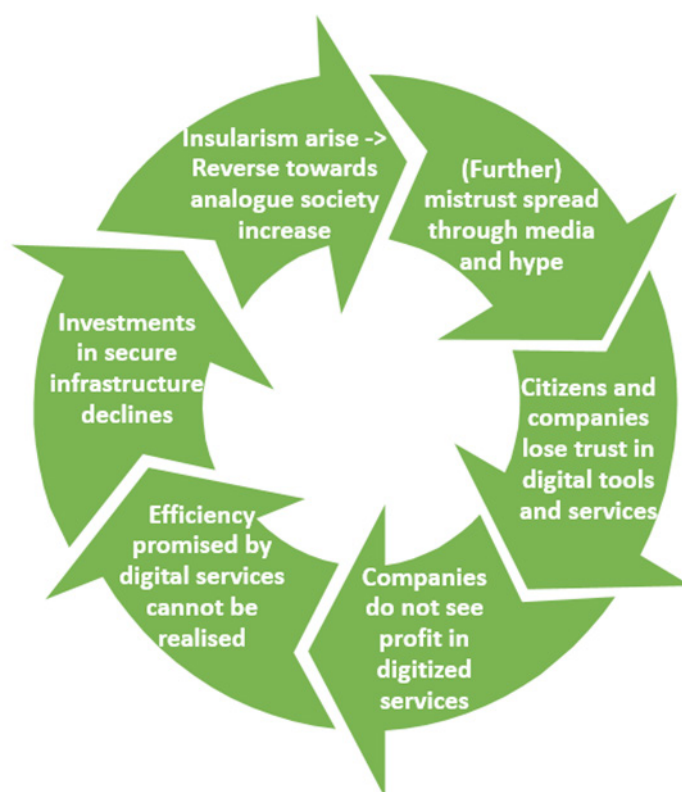
<sup>10</sup> <http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1719> Accessed 21 October 2018



in developing nations<sup>11</sup>. Trust seems to decrease in direct proportion to the length of exposure to Internet services and their associated risks.

Overall, across all markets, trust in organizations' use of personal data is eroding, both in terms of security and use. The question is whether there is a tipping point, when the benefits of signing on to a service are outweighed by the risks and potential damage caused by the online presence. As more and more data flows to private and public companies, and the lack of control and transparency grows, we may be in danger of approaching this point. Indeed, should the balance ever tip against the individual, the ongoing digital evolutionary race between cybersecurity, cybercriminals, companies and public authorities has the potential to jeopardize sustainable growth of the digital economy.

Figure 2 – The circle of mistrust (Wernberg 2007)<sup>12</sup>



'The circle of mistrust' (Figure 2), coined by Wernberg-Tougaard, the Danish global cybersecurity expert, shows how trust in the digital service society can erode, as users turn their backs on the digital economy through lack of trust. It can also help to explain users' rejection of emerging digital options in specific areas. If we take the example of the 'Internet of Things', even simple devices coupled to the Internet can gather information about individuals and their habits, or even become a security threat by turning them into backdoors for hackers, making users less willing to hook up new devices to the Internet, and thereby hampering growth in an otherwise promising new market<sup>13</sup>.

A lack of trust can also be detrimental to competition in the digital economy, as people may be less likely to sign up for competing services, such as new social media platforms, if they already have little

<sup>11</sup> <http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1719> Accessed 21 October 2018

<sup>12</sup> [https://link.springer.com/chapter/10.1007/978-3-8348-9418-2\\_9](https://link.springer.com/chapter/10.1007/978-3-8348-9418-2_9) Accessed 21 October 2018

<sup>13</sup> In 2016 the operation of a number of Internet services was disrupted by the Mirai attack, which utilized a weakness in the communication protocol of millions of web-cameras to create a massive BOT-network. The malware still operates, as the BBC reported on 14 August 2018: <https://www.bbc.co.uk/news/technology-44564709> Accessed 21 October 2018

or no trust in existing platforms. In so doing, they may inadvertently consolidate and promote existing monopolies in online services.

While we do not know where the ‘tipping point’ is, it is nonetheless clear that security and privacy are integral to maintaining and powering the digital economy.

## 2.3 Empowering the app economy

The lack of trust is in contrast with the increased use of Internet-based services, and the increasing global dataflow. In 2018, almost half the global population – more than 3.4 billion people – own a smartphone<sup>14</sup>, and there were more than 4.2 billion active mobile broadband subscriptions worldwide at the end of 2017<sup>15</sup>. This is an extraordinary and enormous market for app-based services and the app economy in general.

It is projected that the global app economy will grow almost five-fold from USD 1.3 trillion in 2016 to USD 6.3 trillion in 2021, as the number of app-users increases to upwards of 6.3 billion people<sup>16</sup>. The app-based economy is a highly influential factor in e-commerce growth, with emerging markets largely skipping the step of using personal computers and instead moving straight to smartphones or tablets to access goods and services online, via apps.

The app economy goes far beyond ‘pay-to-play’ apps. The cashless payment app ‘WeChat’, for example, is currently facilitating more than 600 million daily payment transactions in China. The likelihood of using smartphones to make payments is generally higher in emerging markets, such as India and Indonesia, than it is among the developed economies such as Sweden, France and Japan<sup>17</sup>. Apps are increasingly both a direct and indirect enabler of interaction between consumers and providers of goods and services, interactions which are facilitated by personal data.

Unfortunately, however, the smartphone market is also witnessing a steady increase in specialized malware aimed at ordinary consumers. This includes ransomware, which uses encryption to lock away the phone’s contents from the owner, as well as ordinary viruses and other malware aimed at stealing personal data<sup>18</sup>. This creates a great risk for consumers, as a smartphone often contains not only highly sensitive data, but also financial information. In order to be consistently competitive and attractive, companies need to ensure both privacy and security.

Apps do not stand alone, relying on platforms (IOS, Android etc), a smartphone or tablet, a telecom carrier, and, often, different cloud services, which facilitate the use of the apps themselves. These systems and services also collect personal data, and use the apps to collect data as well. Operating systems and cloud services track where you are (localization), and interact with the apps you use, sometimes coming into conflict with principles of transparency and consent (see chapter 4). Connected wearable devices, such as smart watches and fitness instruments, also connect to operating systems and cloud services, potentially forwarding sensitive personal data to other recipients in a non-transparent way. This raises important questions including where the data goes, who receives it, and is it for sale to other private companies?

It is therefore necessary and important to ensure privacy and security across the entire value chain, from the first step of conceptualization through to the telecom carrier. At each step of the value chain,

<sup>14</sup> [https://actonline.org/wp-content/uploads/ACT\\_2018-State-of-the-App-Economy-Report\\_4.pdf](https://actonline.org/wp-content/uploads/ACT_2018-State-of-the-App-Economy-Report_4.pdf) p5. Accessed 24 October 2018

<sup>15</sup> 2017 ICT statistics, ITU World Telecommunication/ICT Indicators database. Available at: [www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx](http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx)

<sup>16</sup> [http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/621894/EPRS\\_BRI\(2018\)621894\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/621894/EPRS_BRI(2018)621894_EN.pdf) Accessed 21 October 2018

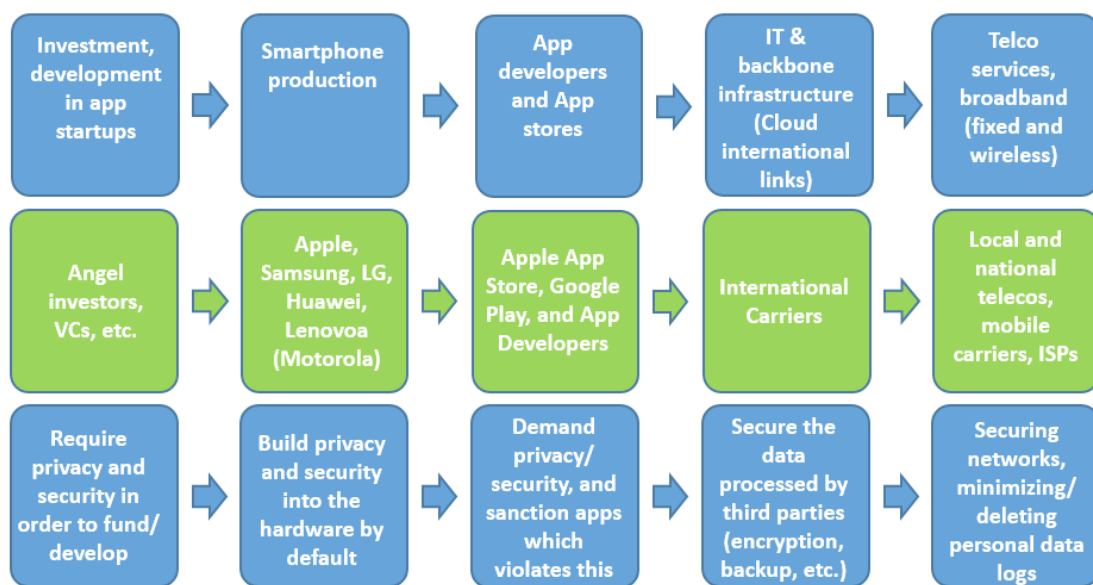
<sup>17</sup> <http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1719> Accessed 21 October 2018

<sup>18</sup> <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf> Accessed 21 October 2018

privacy and security needs to be present and considered (see Figure 2) in terms of Security Design Thinking, Privacy-by-Design and similar holistic lifecycle approaches to security and privacy protection.

For investors and app developers, this means that they need to consider privacy and security at every stage of development, in order to compete and gain consumers’ trust. Indeed, investors should consider requiring privacy considerations in both the business plan and app strategy as a condition for investing, while app-stores can set criteria and conditions for privacy and security. Companies or apps which violate these terms can be sanctioned by being removed entirely from the store.

Figure 3 – App economy value chain (with privacy and security considerations)<sup>19</sup>



From both a financial, business and business ethics point of view, there is a strong case to be made for increasing security and privacy throughout the value chain, as companies can gain competitive advantages and the consumers’ trust by guaranteeing the safety and integrity of their personal data. At the same time, there is also a legal case, as an increasing number of countries pass new privacy legislation, and with GDPR having entered into force (which applies extraterritorially to providers outside the EU – see chapter 4).

Everywhere in the value chain, providers need to understand and control the way data flows between devices and entities. Companies need to be aware of what type of processing the user has given consent to, and then ensure that all future processing is in line with this consent. This includes control over their own data processors (other companies who do data processing on their behalf), as well as control over simple elements such as website cookies.

Ideally, they need to have a full overview of the complete dataflow and all systems where they store personal data, so that they are ready to delete this data whenever consent is withdrawn, or when data is no longer needed. If companies fail to do this, they are also failing to safeguard personal data, as it will be beyond their control.

## 2.4 Digital identities

Successful digitalization between users and the private market and public sector is, to a large extent, built on a combination of trust and convenience. As long as the convenience outweighs the risks, citizens and consumers alike will continue to use specific services.

<sup>19</sup> ITU, The app economy in Africa: Economic Benefits and Regulatory Directions, 2017 and ITU, Regulatory challenges and opportunities in the new ICT ecosystem, 2017.

At the same time as apps are expanding the digital landscape, an increasing number of countries are introducing digital identities as a means to facilitate the digitalization of society, and increase the security and integrity of public and private services online.

A growing number of countries have introduced or are introducing public digital identity systems. In Denmark and Estonia, the government issues digital identities, which can be used to access public services such as welfare, tax, healthcare, and commercial registration, while also facilitating certain private services such as online banking, pensions and much more<sup>20</sup>. While they are using different technologies, their range of services available is quite similar.

In India, more than one billion people have signed up for the Aadhaar digital identity program, making it one of the most successful digital identity programs to date, and securing access to goods, services and governmental programs for a large proportion of the Indian population<sup>21</sup>.

As shown in chapter 5, digital identities have the potential to play a key role in building trust in the digital economy.

## 2.5 Legislative approaches to privacy and competition

With expanding e-commerce, outsourcing and the digital app economy, there has also been a growing need for data protection legislation.

Legislation such as GDPR aims to protect personal data through means of transparency, data controller responsibility, individual rights and security.

Australian legislators have taken a different approach to privacy, however, regulating the use of personal data based on a premise of anti-trust and competition, recognizing that the use of personal data is not just an issue of privacy, security and trust. Personal data is in juxtaposition between being a liability in terms of security and trust, and a commodity which can be used to gain significant competitive advantage.

The Australian Competition & Consumer Commission (ACCC) has a Data Analytics Unit with the specific purpose of ensuring the lawful use of big data and big data algorithms. The ACCC has launched a project which looks into digital platforms (search engines and social media) in competition, including their significance for privacy laws<sup>22</sup>. Further cementing the close tie between competition laws and privacy, the Australian Treasury's proposed new 'Consumer Data Right' will give consumers the right to safely access certain data about themselves which is held by businesses. They will also be able to request this information to be transferred to accredited, trusted third parties of their choice. At first the Consumer data Right will only apply to the banking sector, but later it will be rolled out in other areas on a sector by sector basis<sup>23</sup>.

The Australian Consumer Data Right is very similar to the right to data portability in GDPR, where citizens have the right to receive and transfer their data to and from different controllers, under certain criteria. The big difference between GDPR and the Australian Consumer Data Right is the term 'consumer', which firmly places the right as a competition and consumer issue, with close ties to privacy. Indeed, the main purpose of the legislation is to give consumers control over their own data, hereby promoting competition, and creating opportunities for new ideas and businesses to

<sup>20</sup> For a more in-depth discussion on digital identities, see the 2018 ITU Digital Identity Roadmap Guide and the study on the Digital Identity in the ICT ecosystem: An overview. <https://www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx>

<sup>21</sup> <https://www.uidai.gov.in/> Accessed 21 October 2018

<sup>22</sup> <https://www.accc.gov.au/media-release/new-competition-laws-a-protection-against-big-data-e-collusion> and <https://www.accc.gov.au/system/files/DPI%20-%20Issues%20Paper%20-%20Vers%20for%20Release%20-%2025%20F.%20-%20%28006%29.pdf> Both accessed 21 October 2018

<sup>23</sup> [https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983\\_consumer-data-right-booklet.pdf](https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf) Accessed 21 October 2018

emerge and grow, while also securing security and privacy<sup>24</sup>. This is reinforced by the fact that both the ACCC and the Office of the Australian Information Commissioner (OAIC) will be responsible for the enforcement and development of the Consumer Data Right.

Individual rights such as the Consumer Data Right and the right to data portability in GDPR open the opportunity to break online monopolies, by ensuring that consumers can change providers without necessarily having to start from scratch. This ensures that broken trust in a specific service provider does not necessarily translate into a choice between staying or completely rejecting the service, but rather gives the option to choose a different provider, without suffering penalties.

As explored further in chapter 4, legislative approaches to the digital economy have the potential both to empower or to hinder growth in the digital economy.

## 2.6 The right to be anonymous?

All of this raises the question: should users have the right to be anonymous online? This is not an easy question to answer. As stated earlier, personal data is the primary fuel which drives the digital economy, and as such is deeply integrated into most online services. It is also clear that many online businesses will need personal data in order to deliver their services. It is not possible for online shops to ship merchandise, for example, unless they have name and address details for shipping. Other companies also need proof of the existence of buyers and physical people in order to comply with anti-money laundering legislation and national taxation rules.

New technologies, such as Blockchain (covered further in chapter 6), might help to make anonymity more possible in the not too distant future, but this may also require legislative action.

Currently, we are not therefore at the point where total anonymity in all consumer interactions on the Internet can be made possible. However, as we approach the tipping point of what is possible at a technical level, the possibility of complete anonymity could be nearer than we think. But any such right to anonymity will have to be balanced carefully with national security.

<sup>24</sup> See [https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983\\_consumer-data-right-booklet.pdf](https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf), p1, "Four Key Principles" Accessed 21 October 2018



### 3. Understanding online data business models and data markets

There is no doubt that data has become one of the most valuable commodities in the world, riding the wave of increased digitalization. Companies such as Amazon, Apple, Facebook and Google dominate the top of the list of the world's most valuable companies, leading some to proclaim that data is the new oil<sup>1</sup>. While oil and data are both vital to the global economy in the 21<sup>st</sup> century, there are a number of key differences that make this comparison somewhat misleading.

Firstly, oil is finite and physical, and its value has steadily climbed over the last century as demand has increased and availability diminishes. By comparison, data is infinite; we are constantly creating more and more data, both actively and passively. This will grow even faster as ever more people come into contact with data-producing activities and devices.

Secondly, oil as a tradable commodity suffers from a major vulnerability in being expensive and slow to transport. It is also susceptible to global friction as oil tankers and pipelines cross international boundaries and can often become early targets in times of conflict. Data by comparison can be sent near-instantly, and it can be duplicated. It takes weeks to send a barrel of oil from Denmark to Vietnam, but only a second to send a digital picture of that same barrel of oil to people in twenty countries around the world.

#### 3.1 Data and the two-sided marketplace

In traditional sales, a company sells a product to a customer. The product may have been created by the company or acquired by the company from a manufacturer. When the commodity being sold is a service, the company will normally either be the provider of that service or act as an agent, selling the service on behalf of another company.

<sup>1</sup> <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>  
Accessed 21 October 2018

The two-sided market, looking particularly at the use of apps, is revolutionizing not only the way that we carry out transactions, but also what products and services we now have access to, and, crucially, the pricing.
























In order to examine the differences between a conventional marketplace and an app-based two-sided market, it is worth looking at the impact of the ride-hailing app ‘Uber’ compared with the conventional taxi business model.

Uber, launched in 2011 from its predecessor Ubercab, now operates in 300 cities in 59 countries. In linking drivers with cars to customers requiring transport, it is a classic example of a two-sided app-based economy. Uber does not own the cars, and the drivers are not employees in the traditional sense that they are paid wages by Uber, nor are the vehicles they use run and maintained by Uber. The business model is fundamentally different from that of a conventional taxi company that has to procure, maintain and insure a fleet of cars – cars which are not efficient when not in use. The Uber model outsources the costs and simply takes a percentage of the payment when a vehicle is used. In terms of efficiency, Uber has offloaded all of the inefficient parts of the model onto the driver.

Comparably, Airbnb performs a similar two-sided app-based service. In matching people requiring accommodation and those willing to provide it on a commercial basis, it replicates a conventional industry (hotel booking), but without the significant infrastructure and staff costs that come with a conventional hotel business.

The explosion in the two-sided app-based economy has been facilitated by advances in mobile phone technology. Previously, in order to create and use a two-sided service, such as a taxis or accommodation, you would need a number of different tools available to you. Mobile phones however concentrate many disparate features into a single device which is connected to the digital world, as shown in Table 2.

Table 2 – Mobile phone feature usage in passive and active data collection.

Feature	Airbnb	Facebook	Netflix	Uber	Alibaba.com
App					
GPS					
Payment					
Messaging					
Camera					
Media Viewer					

### 3.2 How do these apps make their money?

As we have seen with Uber, a common method of securing revenue is to take a percentage of the financial transaction between the parties on either side of the app.

However, there are a number of other ways that vendors in the digital market place, supported by apps, secure revenue.

## Airbnb

Airbnb is a defining success story of the two-sided economy, having started in 2008 and posting profits of USD 93 million<sup>2</sup> and total revenue of USD 3.5 billion<sup>3</sup> in 2017. In order to do this, Airbnb, using its website or app, matches people who have a room or a property to rent out and clients who are looking for somewhere to stay. The company charges the property owners a 10% commission while also charging those making the booking a 3% transaction charge.

## Facebook

By most units of measure, Facebook is the most successful example of an app-focused organization. Despite a difficult year in 2017, with numerous scandals regarding data manipulation, Facebook still secured a significant growth in profit (61%)<sup>4</sup>, largely due to an increased user base. As barriers to owning and using smartphones are constantly lowered, particularly in Africa and Asia, Facebook access via a smartphone app has enabled the company to reach an ever higher proportion of the global population, particularly where mobile networks provide the only Internet access infrastructure.

So how does Facebook generate money? Despite the misconception that Facebook sells personal data to advertisers, the reality is that they provide a much more bespoke service, matching advertisements to potentially interested customers. Here, Facebook CEO Mark Zuckerberg explains the process to the Senate Judiciary and Commerce Committees' joint hearing, regarding the company's use and protection of user data, on Capitol Hill in Washington<sup>5</sup>:

*"What we allow is for advertisers to tell us who they want to reach, and then we do the placement. So, if an advertiser comes to us and says, 'All right, I am a ski shop and I want to sell skis to women,' then we might have some sense, because people shared skiing-related content, or said they were interested in that, they shared whether they're a woman, and then we can show the ads to the right people without that data ever changing hands and going to the advertiser."*

## Netflix

Another method of generating income is the more traditionally recognized subscription for service model, whereby customers pay a recurring fee to secure access to a commodity. Netflix, with almost 120 million members in over 190<sup>6</sup> countries dominates this field, with customers choosing from various subscription levels to access services. The technological abilities of mobile phones, along with increasing connection technologies such as 4G/5G mean that streaming content now occupies a significant share of app-based data use.

### 3.3 Who controls your data?

Data, like any commodity in a competitive market place, has value. Organizations that rapidly acquire and manage relevant data will, at worst, have a better understanding of their market, and at best have a valuable commodity they can monetize by selling it on to the highest bidder – and which they can continue to resell over time.

<sup>2</sup> <https://nordic.businessinsider.com/airbnb-profit-revenue-2018-2?r=US&IR=T> Accessed 21 October 2018

<sup>3</sup> <https://www.ft.com/content/96215e16-0201-11e8-9650-9c0ad2d7c5b5> Accessed 21 October 2018

<sup>4</sup> <http://fortune.com/fortune500/list/filtered?sortBy=profits&first500> Accessed 21 October 2018

<sup>5</sup> <https://nordic.businessinsider.com/how-facebook-makes-money-according-to-mark-zuckerberg-2018-4?r=US&IR=T> Accessed 21 October 2018

<sup>6</sup> <https://www.forbes.com/sites/danafeldman/2018/01/22/netflix-has-record-breaking-fourth-quarter-in-2017-exceeds-11b-in-revenue/> Accessed 21 October 2018



One of the side effects of this is a growing number of court cases and high profile data scandals across the globe. Governments meanwhile are trying to adapt and update their data protection laws and regulations quickly in order to keep up with the rapid changes occurring in the fast-paced data market. But to be effective, especially across international boundaries and areas of data sharing, we must first address what data we are talking about and who owns it.

Over the past year, Facebook has been embroiled in data protection legal and regulatory disputes, primarily focused on the use of its users' personal data. The most high profile case concerns the accusation that Facebook allowed the harvesting of the personal data of 87 million users and that this was shared and used by Cambridge Analytica, a data mining and brokerage firm. Below is an extract from the UK's ICO, following an investigation into the misuse of personal data<sup>7</sup>:

*"The ICO's investigation concluded that Facebook contravened the law by failing to safeguard people's information. It also found that the company failed to be transparent about how people's data was harvested by others."*

The current focus on data ownership has provided some clarification on the data flow chain between the data owner, companies, and organizations that may wish to use it. Under GDPR, individuals (the data subject) are the inherent owners of their own personal data. The regulation makes it clear that while the data subject retains ownership of their data, data controllers and processors can use personal data, as long as a set of principles are adhered to (see chapter 4).

The Facebook case demonstrates the increase in data-protection compliance requirements. In the UK, Facebook was fined GBP 500,000 (the maximum fine permissible at the time) for two breaches of the 1989 Data Protection Act, as the offences took place during the tenure of the Data Protection Act. Had they taken place after 25 May 2018, when GDPR came in to force, the fine could have been more than 30 times higher.

### 3.4 Data ownership, privacy and competition considerations

The question of who owns your data is also related to questions concerning competition and anti-trust laws. The value of ICT companies depends not only on the technology but also on the number of users. In 2014, Facebook acquired the messaging app WhatsApp for USD 19 billion. The technology offered by WhatsApp is a relatively simple instant message technology, which Facebook could easily have duplicated or provided via a competing messaging service. The price however was based not on the technology, but on WhatsApp having more than 600 million users around the world<sup>8</sup>. In effect, Facebook was buying the user base, facilitating a transfer of 'ownership', or rather 'controllership' of the personal data. With WhatsApp, Facebook acquired not only the rights to the usage of personal data, but also the legal obligations under various data protection regimes.

From a data protection point of view, this is an issue, as users gave consent to one type of data processing under the previous owners, but are likely to have their data processed differently and used for other purposes by the new owners. This creates a potential multitude of legal compliance issues.

Another competition-related issue is the amount of personal data held by a single company. When a company such as Facebook buys the largest providers of digital services, such as WhatsApp and Instagram, questions of monopoly and dominant market position start to arise. How much personal data may a single company control before anti-trust laws start to apply?

<sup>7</sup> <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/> Accessed 21 October 2018

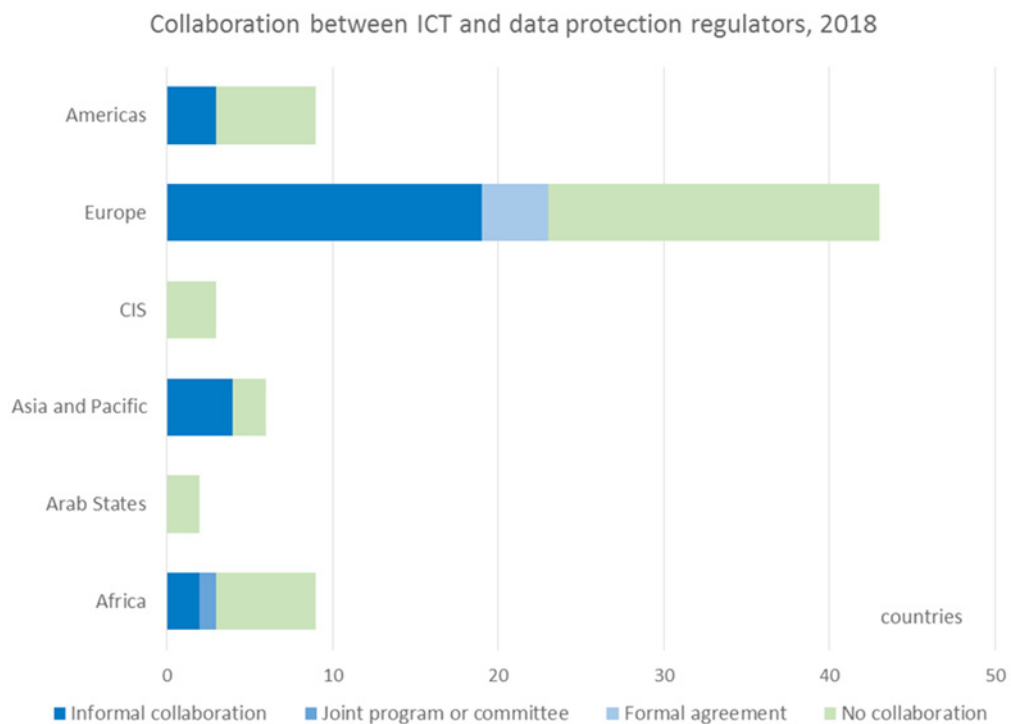
<sup>8</sup> <https://www.forbes.com/sites/parmyolson/2014/10/06/facebook-closes-19-billion-whatsapp-deal/#3a8740d05c66> Accessed 21 October 2018

We are beginning to see anti-trust regulations being applied in this area. In 2018, the EU Commission fined Google more than EUR 4 billion for illegal practices regarding the use of its Android platform. The Competition Commissioner found that Google had required manufacturers to preinstall the Google Search and Google app with exclusivity, thereby preventing the sales of Android devices with other preinstalled apps<sup>9</sup>. In its decision, the EU Commission emphasized the fact that Google Android already had more than 80% of the global smartphone operating system market. Google, by closing the market for preinstalled apps other than its own, abused its dominant market position.

While the decision did not emphasize the use of personal data, there can be no doubt that with these developments, as well as those seen in Australia, there will be an ever-increasing focus on personal data and competition. The question remains of how many users a company can have before it is considered to have attained a dominant market position? This is not an easy question to answer, and will become increasingly relevant in the future.

Such questions will impact the work of data protection regulators, anti-trust regulators, and ICT regulators. Although we are currently seeing cooperation between competition and data protection authorities (DPAs), there is much less between DPAs and ICT regulators. Indeed, analysis conducted by ITU<sup>10</sup> concluded that there is very little cooperation between ICT regulators and DPAs for the time being. Regulatory collaboration has proven possible between the two regulatory agencies in only 33 countries, and the majority of those collaborate only informally. Formal and semi-formal collaboration – either through an agreement or a joint committee– represents only 3% of countries worldwide, leaving more than half of the existing DPAs with no form of collaboration with the ICT regulator at all.

Figure 4 – Collaboration between ICT regulators and Data Protection Authorities



Note: This is based on 72 countries where separate agencies exist and have data protection/privacy measures within their mandate. In addition, in seven countries data protection falls within the mandate of one agency either as sector specific, converged or multisector regulator.

Source: ITU

<sup>9</sup> [http://europa.eu/rapid/press-release\\_IP-18-4581\\_en.htm](http://europa.eu/rapid/press-release_IP-18-4581_en.htm) Accessed 21 October 2018

<sup>10</sup> Global ICT Regulatory Outlook 2018, ITU.

This is an important missed opportunity, given ICT regulators' sector specific expertise and technical knowledge. As mentioned earlier, privacy considerations are very much relevant across the entire ICT sector. The DPA in Singapore has issued guidelines for data protection in telecoms, which encompass questions such as roaming and subscriber identity for call and text messages etc<sup>11</sup>.

With the size of the digital economy, and the increasing focus on privacy legislation, there is a real need for DPAs and ICT regulators to work together, to help facilitate industry standards and collaborate in creating meaningful co-regulation (see chapter 4).

### 3.5 What are the pressure points?

One of the defining characteristics of the digital economy – and one of the main reasons for its success – is the boom in the production and use of data. Any threats to the supply of data, or restrictions on its use, will therefore have as significant an impact on the digital economy as restricting the flow of oil would have on the conventional economy.

There are two significant pressure points that already need addressing, and both regulators and those processing data need to acknowledge them, and to work towards ensuring continued data flow.

The first major pressure point is individual data owners. Within the EU, very few people will have been immune to the barrage of emails from organizations asking in recent months for permission to continue processing personal data that they hold (and may have held for many years). In many ways this has removed the 'blissful ignorance' we have lived with concerning how much personal data we have already freely or unwittingly given away. Most of us have consumed an ever-increasing amount of free online services without considering that there has been a price to pay in terms of personal data. On balance, and in light of frequent data breach news reports, there will be those who now decide they want to drastically reduce or even eliminate their online presence, along with the data they share. If enough people do this, it would ruin any company depending on that data. There is growing evidence that companies that are seen to act against our best interests with regards to personal data will be affected – and it is interesting to note that just 51% of US teenagers say that they use Facebook in 2018, down from 71% in 2015 – although many have moved to Instagram, which is also owned by Facebook<sup>12</sup>.

The second pressure point, following directly on from the first, is the regulatory response to heightened concerns over the use of data. Regulators looking to assign responsibility and controls, along with financial penalties for non-compliance, have created problems for companies whose business model relies on data (this is covered in more detail in chapter 6, which examines barriers to securing data and data compliance). With GDPR setting such high levels for financial penalties, companies affected by it – and these are not only limited to EU-based companies – are having to divert resources into understanding and implementing additional controls. At the same time they risk losing revenue as a more wary public begins to withhold more and more data. In addition, there is now a wider public understanding that companies must also delete personal data under the 'right to be forgotten' principle of GDPR.

The stormy mixture of compliance and awareness must be navigated carefully. Companies not taking active measures to assure data subjects that their personal data will be safe with them *will* now start to face consequences. As seen below, one of the world's most data-dependent companies is starting to feel direct pressure points from both regulation and diminishing data subject trust<sup>13</sup>:

<sup>11</sup> <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/finalised-advisory-guidelines-on-application-of-pdpc-to-telecom-sector.pdf> Accessed 21 October 2018

<sup>12</sup> <https://www.theguardian.com/technology/2018/jun/01/facebook-teens-leaving-instagram-snapchat-study-user-numbers> Accessed 20 October 2018

<sup>13</sup> [https://www.business-standard.com/article/international/facebook-s-next-privacy-challenge-118080201659\\_1.html](https://www.business-standard.com/article/international/facebook-s-next-privacy-challenge-118080201659_1.html) Accessed 21 October 2018

*‘Facebook said Europe’s new privacy law — General Data Protection Regulation, or GDPR — contributed to slowing revenue growth in its quarterly earnings report on Wednesday, which sent its shares plunging nearly 20% over Thursday and Friday.’*

### 3.6 Openness and trust

In the US, a 2018 survey found 78% of respondents said that a company's ability to keep their data private is ‘extremely important’<sup>14</sup>. Companies that can demonstrably show they understand this and take the issue seriously will naturally move ahead of their competitors in the race for customers. As such, openness and trust should emerge in boardrooms around the world as a key opportunity to exploit, rather than seeing data protection as another regulatory hoop which organizations must jump through.

But how best to do this? Deloitte’s report ‘Building Trust across Cultures’<sup>15</sup> says that organizations should seize the opportunity to treat privacy and data protection as a separate stream or additional feature, thereby ‘building a better a relationship with their consumers, making sure that their customers become a key part of the brand’.

The report highlights five key steps to achieve this:

**Table 3 – Building trust across cultures**

Step	Activity
Regulators take a more proactive approach to privacy and data regulation.	Evolving technologies and shifting global and regional views on data protection.
Building a sustainable privacy framework.	A framework that works across an increasingly complex data landscape can tolerate emerging risks and expectations of data subjects, regulators, third parties and global and cultural expectations.
Understanding the consumer angle.	Consumers are now aware that their data is their property and are more informed about their data rights. Organizations will be increasingly expected to meet consumer demands, so understanding them is crucial.
Third and cross-party management.	Data protection and risk management must be expanded to incorporate the risks of sharing information with third and cross-parties and be compliant across international borders.
Overcome the fear of transparency.	Organizations may fear that honesty and transparency regarding how they use personal data will draw unwanted attention to their data activities, driving customers away. This must be overcome to build trust with consumers, ensuring longer-term customer loyalty.

<sup>14</sup> <http://newsroom.ibm.com/Cybersecurity-and-Privacy-Research> Accessed 21 October 2018

<sup>15</sup> <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-building-trust-across-cultures.pdf> Accessed 20 October 2018



#### 4. Models of ensuring protection, privacy and trust

A growing global dataflow and the expanding use of personal data in the global economy have led to an increase in the adoption and development of national and regional privacy laws and regulations. The principle motives for this are a wish to secure the fundamental human right to privacy, and the wish to protect consumers and promote competition. Whichever motive is behind national legislation, most modern privacy regimes find common origins in universal human rights, and in particular the right to respect for private and family life<sup>1</sup>.

There can be no doubt, however, that these developments have the potential either to disrupt the global dataflow and stifle the digital economy, or to promote and energize it.

UNCTAD, in a 2016 report<sup>2</sup>, warned that overregulation might hinder global growth, and called for a fair balance between international trade and privacy considerations. It also warned that divergent in data protection regulation at regional and national levels might hinder the growth of digital markets.

The closest candidate for a global treaty is the Council of Europe Convention 108 on data protection, which currently has six non-Council of Europe member countries as parties to the convention (Cape Verde, Mauritius, Mexico, Senegal, Tunisia and Uruguay). Argentina, Burkina Faso and Morocco currently have accession requests waiting<sup>3</sup>. Convention 108 was updated in May 2018, in order to modernize the convention in the wake of GDPR<sup>4</sup>.

At the same time, OECD guidelines from 1980 are still being referred to in modern privacy frameworks, such as APEC, making them a strong contender for a universal data protection framework.

The APEC data protection system differs greatly from the EU system, as there is no legally binding treaty, but rather a set of privacy guidelines (*APEC Privacy Framework*), based on the OECD guidelines from 1980. In 2012, ASEAN (the Association of South-East Asian Nations) similarly adopted a regional

<sup>1</sup> [http://fra.europa.eu/sites/default/files/fra\\_uploads/fra-coe-edps-2018-handbook-data-protection\\_en.pdf](http://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf) Accessed 21 October 2018

<sup>2</sup> [http://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf) Accessed 21 October 2018

<sup>3</sup> <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures> Accessed 21 October 2018

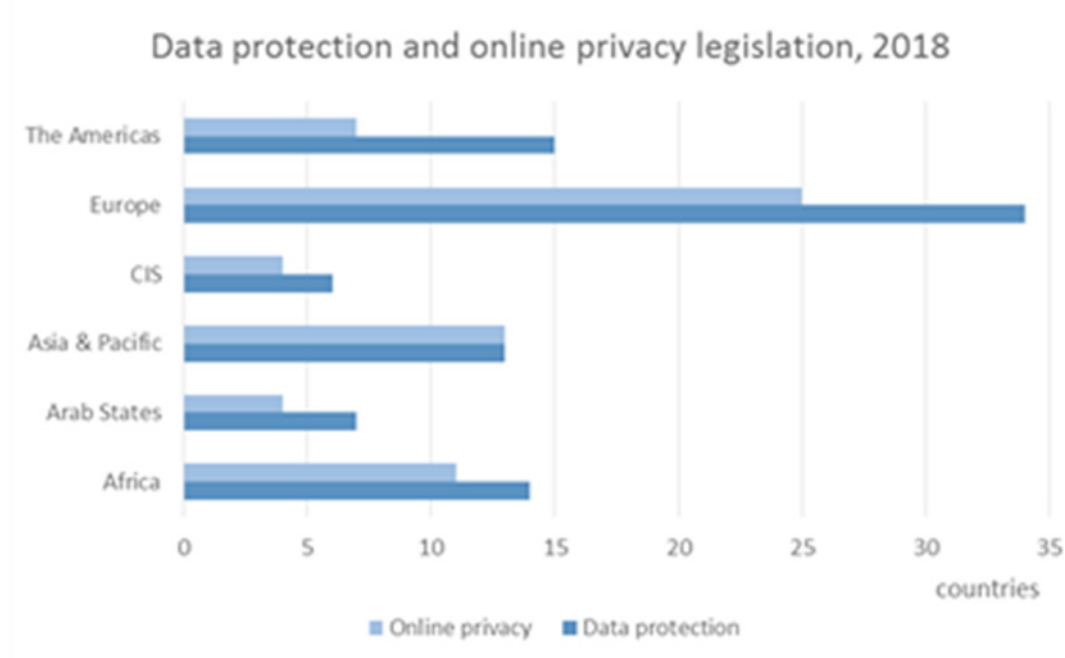
<sup>4</sup> [https://search.coe.int/directorate\\_of\\_communications/Pages/result\\_details.aspx?ObjectId=0900016808ac976](https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900016808ac976) Accessed 21 October 2018

*Framework on Personal Data Protection*, which is compatible with the APEC framework (some countries are members of both ASEAN and APEC).<sup>5 6</sup>

Some countries have Data Protection Authorities (DPAs), while others do not, and some countries have no legislation at all. Others may have sector specific legislation, but no economy-wide data protection regulations such as GDPR, which applies both horizontally and vertically. In many countries around the world, there is a strong global trend however towards the establishment of special data protection authorities with strong enforcement powers<sup>7</sup>. Globally, around 60% of countries have now set up a DPA. Europe and Asia-Pacific are ahead of other regions in this regard, having a large majority of countries with a mature – or at least maturing – institutional framework. In other regions, the trend has yet to gain the same momentum<sup>8</sup>.

At least 109 countries around the world have adopted some form of data protection and privacy legislation<sup>9</sup>. While 10% of countries have draft legislation, 21% have no legislation whatsoever<sup>10</sup>.

Figure 5 – National data protection and privacy by region (ITU) and worldwide (UNCTAD)<sup>11</sup>



Source:ITU

<sup>5</sup> <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> Accessed 21 October 2018

<sup>6</sup> See also ITU's GSR-16 discussion paper on maintaining trust in a digital connected world, at: <https://www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx> Accessed 21 October 2018

<sup>7</sup> See the interactive map of the French data protection authority *Commission Nationale de l'Informatique et des Libertés* (CNIL) for a full list of countries: <https://www.cnil.fr/en/data-protection-around-the-world> Accessed 21 October 2018

<sup>8</sup> ITU Global ICT Regulatory Outlook, 2018 and ICT Regulatory tracker 2017.

<sup>9</sup> ITU Global ICT Regulatory Outlook, 2018.

<sup>10</sup> See: [https://unctad.org/en/Pages/DTL/STI\\_and\\_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx](https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx)

<sup>11</sup> See [http://unctad.org/en/Pages/DTL/STI\\_and\\_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx](http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx). Screenshot of map provided by UNCTAD. Accessed 21 October 2018

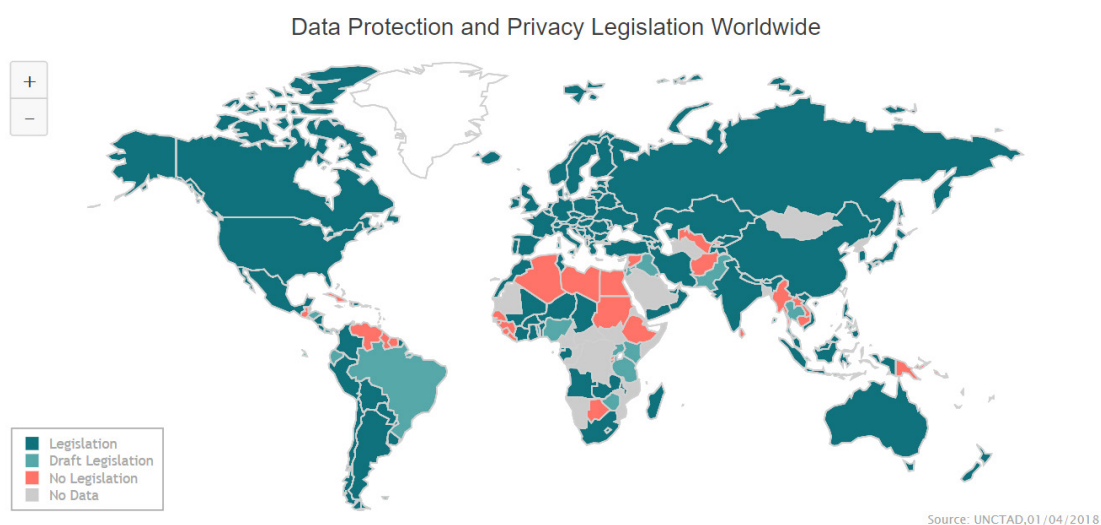


Table 4 – Core Data Protection Principles (UNCTAD)

1. <b>Openness:</b> Organizations must be open about their personal data practices.	5. <b>Security:</b> Personal data must be subject to appropriate security safeguards.
2. <b>Collection limitation:</b> Collection of personal data must be limited, lawful and fair, usually with knowledge and / or consent.	6. <b>Data quality:</b> Personal data must be relevant, accurate and up-to-date.
3. <b>Purpose specification:</b> The purpose of collection and disclosure must be specified at the time of collection.	7. <b>Access and correction:</b> Data subjects must have appropriate rights to access and correct their personal data.
4. <b>Use limitation:</b> Use or disclosure must be limited to specific purposes or closely-related purposes.	8. <b>Accountability:</b> Data controllers must take responsibility for ensuring compliance with the data protection principles.

While countries adopt different types of legislation, data protection regimes are usually a set of core principles, whose origins go back to the OECD guidelines from 1980. UNCTAD has identified eight core principles, which can be found in some form or other in most local and regional agreements and guidelines<sup>12</sup>. These are shown in Table 4.

#### 4.1 Understanding EU GDPR

On 25 May 2018, EU GDPR came into force in all 28 EU member states. Compliance with the new regulation has been estimated to cost over USD 9 billion for Fortune 500 and FTSE 350 companies<sup>13</sup>. While the new regulation and the old EU directive share much of their content and principles, GDPR is much stricter, placing fines on companies of up to 4% of global revenue or EUR 20 million (whichever is highest), and increasing the legal requirements and accountability for data controllers and data processors.

<sup>12</sup> [http://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf). See p. 56 – 57, including table contents and figure. Accessed 21 October 2018

<sup>13</sup> <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#73a10aaa34a2> Accessed 21 October 2018

GDPR also regulates the different responsibilities of the data controller in greater detail than the earlier directive. These include the responsibility to: comply with individual rights; guarantee adequate data security based on a risk assessment; conduct Data Protection Impact Assessments (DPIAs); keep records on the types of processing conducted; notify supervising authorities and data subjects in the event of a data breach; and appoint a data protection officer (if certain requirements are met).

GDPR contains an accountability requirement, where a controller and processor must also be able to demonstrate compliance with GDPR requirements by providing adequate documentation on request by supervising authorities.

In 2017, the UK's ICO found that the Royal Free NHS Foundation had violated the UK's national data protection act by forwarding 1.6 million health records to Google DeepMind for analysis. This transfer was a violation of individuals, and ICO commented that:

*'Privacy impact assessments are a key data protection tool of our era, as evolving law and best practice around the world demonstrate. Privacy impact assessments play an increasingly prominent role in data protection, and they're a crucial part of digital innovation. Our investigation found that the Trust did carry out a privacy impact assessment, but only after Google DeepMind had already been given patient data. This is not how things should work.'*<sup>1</sup>

<sup>1</sup> <https://ico.org.uk/about-the-ico/news-and-events/blog-four-lessons-nhs-trusts-can-learn-from-the-royal-free-case/> Accessed 21 October 2018

While independent supervising authorities in each member country are responsible for oversight and enforcement, GDPR means that consumers are now likely to play a more important role than before. With GDPR, individual rights have expanded, and the right to transparency means that data controllers are required to inform their data subjects about their rights, as well as about the obligations of the data controllers themselves.

Aside from GDPR, each country also has its own data privacy laws, which regulate selected areas of data protection, which GDPR leaves to member states, including sector specific legislation, which may regulate specific privacy issues.

As mentioned earlier, consumers are already well aware of these changes in the rules, as their inboxes have been flooded with privacy notifications from companies preparing for GDPR, and the regulation has had considerable coverage in the media. With consumers now having the right to complain directly to supervising authorities, we are likely to see significant impacts from this new paradigm of European data protection.

While GDPR could be perceived as being a burden on companies, it may also help increase consumer trust in the digital economy, as consumers become more aware of the rules for data protection, their own rights, and the requirements for transparency in the processing of personal data.

It is worth noting however that GDPR is not the only model which exists for data protection regulation; other models will be examined in section 4.3.

## 4.2 What does EU GDPR mean for citizens?

Under EU GDPR, citizens benefit from many regulations aimed at protecting their individual rights concerning their personal data<sup>14</sup>.

<sup>14</sup> Not all of these rules are new; some were also present under EU directive 95/46/EC



The right to be forgotten is now enshrined in GDPR. When an individual requests this, or the data is no longer needed, the data controller is required to completely delete all data about the individual, if there are no legitimate grounds for further retention.

Citizens have the right to access their personal data, as well as to request the limitation or minimization of it. They are required to be informed how the data is processed, what the legal basis is, and who receives the data, among other things. When a new controller receives personal data, they are also required to give notice thereof to the respective individuals.

When data breaches occur which are likely to have a high risk for individuals, those individuals also have the right to be notified as quickly as possible, without undue delay.

Certain types of entities are required to appoint a Data Protection Officer, who must offer independent help and guidance to individuals regarding the enforcement of their rights, and help their respective organizations with data protection compliance.

Data protection by design and default is now an integral part of the data protection regime, with the requirement that privacy is built into new products and services from the very beginning, instead of only being implemented later. This is likely to affect the mobile app market and social media platforms in particular.

IT and information security is now an integral part of the legal requirements. A risk-based approach to the protection of personal data needs to include the adoption of technical and organizational safeguards, which are adequate for the protection of the type of data processed. This includes, but is not limited to, encryption, pseudonymization and anonymization. The confidentiality, integrity and accessibility of EU citizens' personal data is now a legal requirement for all controllers and processors of data.

The rules for processing data on children have been tightened, and the need for correct consent from a parent or guardian is emphasized.

GDPR also places restrictions on cross-border data transfers, guaranteeing that data is not sent out of the EU without the adoption of appropriate safeguards<sup>15</sup>.

### 4.3 Different models for data protection regulation

Three different types of regulation are identified by Professor Dennis D. Hirsch: direct regulation, self-regulation, and co-regulation (which can be similar to collaborative regulation between the private sector and the regulator<sup>16</sup>). Each of these has three different applications, and they can be applied at three different levels: at the level of each individual company; sector wide (a specific type of sector, or the private sector only); or to the economy as a whole (including both the private and public sectors). This creates nine different combinations for regulatory design<sup>17</sup>.

<sup>15</sup> See also from the EU commission: [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf) Accessed 21 October 2018

<sup>16</sup> For more information on the concept of collaborative regulation, see ITU's Global ICT Regulatory Outlook 2017 and the 2018 edition, available at: [www.itu.int/treg](http://www.itu.int/treg).

<sup>17</sup> These models for thinking about data protection regulation types are an adaptation of the work of Dennis D. Hirsch, and not a direct application of his models. There are therefore certain derogations within this report. See: Hirsch, Dennis D., In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct (December 1, 2013). Ohio State Law Journal, Vol. 74, No. 6, 2013. Available at SSRN: <https://ssrn.com/abstract=2393757> Accessed 21 October 2018

Table 5 – Regulatory design options

	Direct government regulation	Self-regulation	Co-regulation
Company	1*	4	7
Sector	2	5	8
Economy as a whole	3	6	9

\*For the purpose of this report, combination #1 will not be discussed, as government regulation of a single company (singular legislation) falls outside its scope.

#### A. *Direct Government Regulation*

Direct government regulation occurs where national governments create and monitor compliance with the regulations in question. These rules can be based on international treaties, regional frameworks, or other agreements between or within states. From a global point of view, this would be facilitated by incorporating a general international treaty on data protection directly into national legislation.

GDPR is an example of direct government regulation, which applies to the economy as a whole, placing it firmly within combination #3, above; the most common type of regulation on a worldwide basis. The strength of economy-wide direct government regulation is the consistent legal guarantee afforded to consumers. Its downside is that it may be unable to keep up with technological developments, and developments in services across sectors, leaving it liable to become quickly outdated.

In the US, privacy legislation is mostly sector-based (combination #2). Rather than one concise general federal bill, there is sector-based legislation for specific areas, such as the Health Insurance Portability and Accountability Act (HIPAA) within the healthcare sector, and the Family Educational Rights and Privacy Act (FERPA) for the educational sector, while yet another separate bill exists for children, with the Children’s Online Privacy Protection Act (COPPA).

At the same time, there also exists privacy legislation in individual states. In total, the United States has at least 20 federal sector-specific laws, and hundreds of laws within the 50 states combined<sup>18</sup>. Some states, such as California, have even adopted consumer privacy legislation aimed at the private sector, and giving a set of rights very similar to those found in GDPR<sup>19</sup>. At the same time, the Federal Trade Commission (FTC) has developed the practice of considering data protection when evaluating deceptive trade practices within the companies it regulates.

These sector-specific regulatory approaches have the advantage of being tailored to specific sectors, but they can, at the same time, make it difficult for citizens and consumers to understand and to get an overview of whether their rights are within this regime. These issues have prompted the Council on Foreign Relations to propose the adoption of a single federal privacy act, in order to avoid the internal division of US data protection laws; something which was also attempted in 2012 with the Consumer Data Privacy Bill of Rights<sup>20</sup>.

#### B. *Self-regulation*

Self-regulation occurs when companies set up their own regulatory frameworks – for example by protecting personal data through specific internal terms and conditions, or by adopting an internal privacy policy. This is often necessary, as privacy regulation can be somewhat vague; one example being retention periods, concerning the length of time personal data can be kept before it has to be deleted. The time limit will vary from company to company, or sector to sector, depending on the

<sup>18</sup> <https://www.dlapiperdataprotection.com/index.html?t=law&c=US> Accessed 21 October 2018

<sup>19</sup> [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375) Accessed 21 October 2018

<sup>20</sup> <https://www.cfr.org/report/reforming-us-approach-data-protection> Accessed 21 October 2018

type of business involved. GDPR and other privacy legislation do provide some direct regulations, but a certain amount of self-regulation is also required in any company or business in order to be able to demonstrate compliance.

The strength of self-regulation is that it can be flexible and able to keep up with industry changes, advances in technology, and new business practices. The problem however is that these self-regulations may still be insufficient, and therefore at best inadequate and at worst illegal.

One example is the Facebook case, concerning Cambridge Analytica. Facebook stated that Cambridge Analytica had violated Facebook's terms of service by not deleting data after it was found that the data had been used for attempted political gain. An investigation by the UK Information Commissioner's Office, ICO, found that Cambridge Analytica, Global Science Research, and a Dr Aleksandr Kogan paid 320,000 Facebook users to take a survey via an app, which they then used to gain access not only to the members' personal data, but also the accounts of their friends, totaling an estimated 87 million Facebook users<sup>21</sup>.

ICO has 'issued Facebook with a Notice of Intent to issue a monetary penalty of GBP 500,000 for lack of transparency and security issues relating to the harvesting of data constituting breaches of the first and seventh data protection principles under the Data Protection Act 1998'. This is the highest amount possible under the 1998 act<sup>22</sup>. So while Facebook had a terms of service contract, which included privacy considerations, these turned out to be inadequate from a legal point of view, making Facebook culpable under privacy legislation.

At the sectoral level, the Network Advertising Initiative (NAI) is a 'Self-Regulatory Code of Conduct' for the online advertising industry. This aims to follow a combination of industry best practice and basic privacy and data protection principles, including 'Fair Information Practice Principles' of notice, choice, transparency, use limitations, data security, access, and accountability<sup>23</sup>. Member companies of the NIA who wish to follow the code may do so under NIA supervision, and the code includes a set of enforcement procedures.

In 2012, the FTC published a report entitled 'Protecting Consumer Privacy in an Era of Rapid Online Change'. This endorsed the development and use of enforceable sector-based privacy self-regulation. The FTC also expressed the will to collaborate on the creation of sector self-regulatory frameworks<sup>24</sup>. It states that adherence to such codes will be viewed favourably in its law enforcement work, but that it would also be seen as deceitful practice if companies do not follow the codes they have signed up for<sup>25</sup>. Under such a regime, companies can still fall short of actual privacy compliance; although transgressions (in good faith) are viewed more favourably by the FTC than if companies had not followed such sector-based self-regulation.

In a similar fashion, the European Data Protection Board (EDPB; formerly the EU article 29 Working Party) has stated that national DPAs, when setting administrative fines, should ensure that 'due account be taken of any best practice procedures or methods where these exist and apply. Industry standards, as well as codes of conduct in the respective fields or profession are important to take into account'<sup>26</sup>.

<sup>21</sup> <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf> Accessed 21 October 2018

<sup>22</sup> <https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal> Accessed 21 October 2018

<sup>23</sup> <http://www.networkadvertising.org/code-enforcement/enforcement/> For the full code, see: [http://www.networkadvertising.org/sites/default/files/nai\\_code2018.pdf](http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf) Accessed 21 October 2018

<sup>24</sup> <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>, p73. Accessed 21 October 2018

<sup>25</sup> <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> Accessed 21 October 2018

<sup>26</sup> [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=47889](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889), p13. Accessed 21 October 2018

The final example of self-regulation is combination #6, covering the economy as a whole, although examples appear to be rare.

### C. *Co-regulation*

Co-regulation occurs when government agencies and private businesses work together to create privacy regulations, either covering individual businesses, or a specific sector. Under co-regulation, governments and industry share the responsibility for drafting, monitoring and enforcing privacy standards.

Co-regulation goes some way towards addressing the limits of self-regulation. Whereas self-regulation does not guarantee compliance with data protection laws on its own, co-regulation aims to combine the strength of industry self-regulation with consumer guarantees which come with direct government regulation.

GDPR is a good illustration of this. While GDPR does apply to the economy as a whole, it also contains general principles which companies need to assess in order to become compliant. One example is the principle of deletion and data minimization. The retention time for stored data will depend on the type of processing the company does, the type of data it processes, and the applicable national legislation, which might require specific retention periods. The actual retention time cannot therefore be standardized across all sectors and companies. As a result, co-regulation helps companies to ensure compliance, and thereby minimizes the risk of their being fined by national DPAs.

Binding Corporate Rules (BCR) provide an example of combination #7, co-regulation for a single company, corporation, or business venture. BCR is an officially approved internal data protection policy in GDPR<sup>27</sup>, and is approved by national DPAs, after consulting the European Data Protection Board. They are 'legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees'<sup>28</sup>. BCR requires that in order to be approved companies must make rules which encompass all the areas of GDPR<sup>29</sup>.

The APEC countries have a similar regime to BCR in the shape of the Cross Border Privacy Rules System (CBPR), which was built with business and consumer trust specifically in mind. Under CBPR, companies may transfer personal data between APEC member countries, after adopting corporate rules for this transfer, and after being officially accredited, under the supervision of national authorities. CBPR, like BCR, contains not just rules on data transfer, but also more comprehensive requirements, including basic principles such as data limitation and retention<sup>30</sup>.

There are currently six participating APEC CBPR system economies: Canada, Japan, Korea, Mexico, Singapore, and the US<sup>31</sup>.

GDPR also contains rules for sector-based co-regulation (combination #8), entitled 'codes of conduct'<sup>32</sup>. Under this provision, associations and other bodies representing categories of controllers or processors can prepare codes of conduct and present them to the competent DPA for approval<sup>33</sup>. Companies can choose whether or not they wish to follow their sector-specific codes of conduct; controllers for their part can use them to demonstrate compliance with GDPR<sup>34</sup>. Companies can also be certified according to approved rules of conduct by approved certification agencies. Codes of

<sup>27</sup> <https://gdpr-info.eu/art-4-gdpr/> Article 4(20)

<sup>28</sup> <https://gdpr-info.eu/art-47-gdpr/>

<sup>29</sup> <https://gdpr-info.eu/art-47-gdpr/>

<sup>30</sup> <https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Rules%20Program%20Requirements.pdf>  
Accessed 21 October 2018

<sup>31</sup> More information can be found at: <http://cbprs.org/default.aspx>

<sup>32</sup> <https://gdpr-info.eu/art-40-gdpr/>

<sup>33</sup> <https://gdpr-info.eu/art-40-gdpr/> (paragraph 5)

<sup>34</sup> <https://gdpr-info.eu/art-24-gdpr/> (paragraph 3)

conduct can be approved within a member state by a national DPA, across multiple member states by the EDPB, or across the entire EU by the EU Commission.

The DPA and the EDPB are required either to approve or make recommendations when receiving an application for codes of conduct, and according to article 40(1), the DPA, EDPB and EU Commission are required to actively encourage the drafting of such codes. GDPR also allows for certification by accredited bodies who check, monitor, and follow up on compliance.

Finally, there is the EU-US Privacy Shield. This is an agreement between the EU and US, whereby companies that have signed up under the Privacy Shield abide by sufficient rules for them to be able to demonstrate the legality of transfer of personal data between the EU and the US.

Companies under the Privacy Shield must self-certify annually in order to remain on the Privacy Shield list. The EU-US Privacy Shield is an open framework, aimed at the private sector, which any company can sign up for (combination #7 and #8).

**Table 6 – Regulatory design options table, with examples<sup>35</sup>**

	Direct Government Regulation	Self-Regulation	Co-regulation
Company	N/A	Privacy Policies	BCR/CBPR/Privacy Shield
Sector	US sector-specific legislation EU national legislation	NIA	GDPR Codes of Conduct/ Privacy Shield
Economy as a whole	GDPR, national legislation etc	ICX <sup>&lt;?&gt;</sup>	GDPR certification

#### 4.4 Adoption of guidelines

A separate category concerns the issuing of national guidelines on data protection by DPAs. Unlike co-regulation, such guidelines are not in and of themselves legally binding either for data controllers or the DPAs themselves, who can change their guidelines as needed. These guidelines do however give a good indication of what DPAs consider to be good practice, and what they will focus on in case of violations.

National guidelines are often issued by DPAs for the economy as a whole, where they focus on the interpretation of certain data protection provisions. One such example is the guidelines issued by the UK's ICO, which has published several guidelines on GDPR, with a focus on specific topics such as consent and individual rights<sup>36</sup>.

Such guidelines can also be sector-specific. In Singapore, the Personal Data Protection Commission (PDPC) has issued non-binding privacy guidelines targeting the telecom, real estate, education, health-care, social service and transport sectors<sup>37</sup>. From a self-regulation perspective, the PDPC has also worked together with industry associations to create sector-specific industry guidelines. Currently, there are two published guidelines targeting life insurance agencies<sup>38</sup>. In this way, the PDPC facilitates compliance and aids the development of best practice across different sectors.

<sup>35</sup> This completed table differs slightly from Dennis D. Hirsch's original model. See: Hirsch, Dennis D., *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct* (December 1, 2013). Ohio State Law Journal, Vol. 74, No. 6, 2013. Available at SSRN: <https://ssrn.com/abstract=2393757> Accessed 21 October 2018

<sup>36</sup> <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/> Accessed 21 October 2018

<sup>37</sup> <https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines/Sector-Specific-Advisory-Guidelines> Accessed 21 October 2018

<sup>38</sup> <https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines/Industry-led-Guidelines> Accessed 21 October 2018

## 4.5 Implications of EU GDPR on other regions, with a special view to Asia

EU GDPR not only has implications for European businesses, but for any business wishing to enter the European market. GDPR has extraterritorial application. This means that *any* foreign company wishing to process EU residents' data in relation to the selling of goods or services is subject to GDPR on the same terms as companies already established in the EU<sup>39</sup>. Such companies are also required to appoint a representative established in the EU. Some companies have chosen to leave the European market as a result, including the Chicago Tribune and LA Times, pending the finding of 'technical solutions' to achieve compliance<sup>40</sup>.

The news industry is far from the only sector where GDPR has implications for businesses, with restrictions on cross-border data flows between the EU and other countries affecting many companies around the world.

According to the European Centre for International Political Economy (ECIPE), there are two types of restrictions on cross-border data flows: strict and conditional. Under strict restrictions data must be stored and processed locally, while under conditional restrictions, cross-border data transfers must meet specific conditions<sup>41</sup>.

Strict and conditional restrictions to cross-border data flow can be classified as follows:

- A. Strict restrictions on cross-border data flows:
  - i. Local storage requirement;
  - ii. Local storage and processing requirement;
  - iii. Ban on data transfer (ie. local storage, local processing and local access requirements).
- B. Conditional restrictions to cross-border data flows:
  - i. Conditional flow conditions apply to the recipient country;
  - ii. Conditional flow conditions apply to the data controller or data processor.

Local storage requirements mean that a copy of the data must at all times be stored locally, while local processing requirements mean that a company must use data centres located within the country. When there is a ban on data transfer, no data may be transferred out of the country, but usually such bans are limited to specific data types, such as healthcare data or critical national security data. Conditional restrictions occur when cross-border transfers must meet certain requirements to be lawful<sup>42</sup>.

While both the APEC and ASEAN frameworks set guidelines for cross-border data protection transfer, they are not as detailed or demanding as GDPR, which has specific rules covering the transfer of personal data to countries outside of the EU. These requirements cover both points i. and ii. in the model presented above, and the conditional flow therefore applies to both the recipient country and to the data processor or controller<sup>43</sup>. A transfer is only legal in the following circumstances:

- 1) The EU Commission has recognized that the importing country's privacy laws provide adequate protection (article 45).

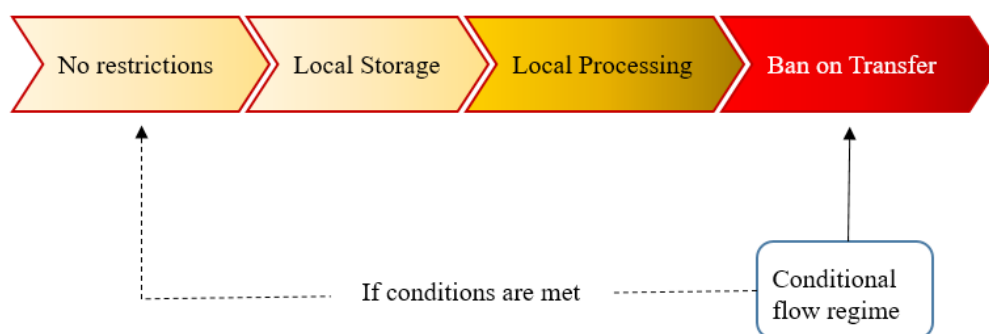
<sup>39</sup> <https://gdpr-info.eu/art-3-gdpr/>

<sup>40</sup> <https://www.marketwatch.com/story/chicago-tribune-la-times-go-dark-in-europe-after-gdpr-fail-2018-05-25> Accessed 21 October 2018

<sup>41</sup> <http://ecipe.org/app/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf> Accessed 21 October 2018

<sup>42</sup> <http://ecipe.org/app/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf> Accessed 21 October 2018

<sup>43</sup> <https://gdpr-info.eu> Articles 44 to 50

Figure 7 – Types of restrictions on cross-border data flows<sup>1</sup>

<sup>1</sup> Figure from <http://ecipe.org/app/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf> Accessed 21 October 2018

- 2) With the adoption of appropriate safeguards, such as binding corporate rules, adoption of standard protection clauses, adherence to approved code of conduct, etc (article 46).

Aside from this, there are also ‘European Essential Guarantees’, which may create a boundary for cross-border data transfers<sup>44</sup>.

Of all the APEC countries, only Canada, New Zealand and the United States (limited to the Privacy Shield framework) are recognized as providing adequate protection, with decisions on Japan and the Korea expected to be adopted before the end of 2018<sup>45</sup>. None of the ASEAN countries are yet recognized, and some have not yet enacted any form of privacy laws.

A few countries with close cultural and historical ties to the European continent, including Australia and New Zealand, passed their first privacy legislation in the 1980s. Other Asian countries passed privacy laws in the mid-1990s, including Korea in 1994, and China, Japan, Hong Kong, China and Taiwan, China in 1995<sup>46</sup>. With GDPR, a number of countries in the region are now choosing to update their privacy laws, including Indonesia, Thailand, and New Zealand, as well as several other countries around the world<sup>47</sup>.

This is likely to be part of the reason why many Asian companies are not yet ready for GDPR. A May 2018 survey from ISACA concluded that less than 30% of Asian companies were ready for GDPR, and less than 40% of the companies surveyed were expecting to be compliant by the end of 2018<sup>48</sup>.

Collectively APEC and ASEAN countries represent a market value of some USD 45 trillion, while the EU represents some USD 19 trillion – but the EU negotiates and acts as a single block, while APEC and ASEAN countries act independently<sup>49</sup>. These figures do not include India, which is a member of neither APEC nor ASEAN.

<sup>44</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf) Accessed 21 October 2018

<sup>45</sup> See [http://europa.eu/rapid/press-release\\_MEMO-18-4503\\_en.htm](http://europa.eu/rapid/press-release_MEMO-18-4503_en.htm) (Japan) and [http://europa.eu/rapid/press-release\\_STATEMENT-17-4739\\_en.htm](http://europa.eu/rapid/press-release_STATEMENT-17-4739_en.htm) (Korea) Both accessed 21 October 2018

<sup>46</sup> See the full list in Greenleaf, Graham, Countries with Data Privacy Laws – By Year 1973-2016 (Tables) (April 2, 2017). (2017) 146 Privacy Laws & Business International Report, 18. Available at SSRN: <https://ssrn.com/abstract=2996139> Accessed 21 October 2018

<sup>47</sup> Id. (Greenleaf)

<sup>48</sup> See ISACA survey at: <http://www.isaca.org/Knowledge-Center/Documents/2018-GDPR-Readiness-Survey-Report.pdf> Accessed 21 October 2018

<sup>49</sup> <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf>, APEC <https://www.apec.org/About-Us/About-APEC/Achievements%20and%20Benefits.aspx>, and the EU <https://data.worldbank.org/region/european-union> All accessed 21 October 2018

With the increasing value of the digital economy, and the promising future of the Asian digital market and digitalization, GDPR should preferably not be a hindrance to global data flow; however, businesses that fail to comply may also fail to realize the full potential of their products and services. Data controllers in Europe could become more reluctant to hire a data controller from Asia for IT outsourcing, while non-EU companies, on the other hand, may – even inadvertently – fail to comply with their legal requirements.

#### 4.6 Data localization, national security and cross border restrictions

Local processing requirements often stem from a wish to protect national interests and security. Privacy considerations for out-of-country processing is a key element of the OECD guidelines, which state that:

*'A Member country should refrain from restricting trans-border flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines (Para. 17)'<sup>1</sup>.*

<sup>1</sup> <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> Accessed 21 October 2018

The OECD guidelines, however, also strongly encourage the adoption of appropriate safeguards.

China has chosen to make data localization a requirement, based on the notion of state sovereignty in cyberspace, and considerations of security and protection. The new Chinese cybersecurity law places a complete ban on the cross-border transfer of 'important' personal data, but makes no clear distinction on what this classification entails – although the government has stated that this requirement will not restrict the dataflow to the detriment of businesses<sup>50</sup>.

In June 2018, the National Assembly in Vietnam passed a new cybersecurity law which requires data of all Vietnamese users to be stored in Vietnam<sup>51</sup>. Russia also has a data localization law, which requires data to be stored in Russia when it originates within the country. The transfer of data is legal under this legislation, however it must only be in copy form, and the 'main database' must be located in Russia.<sup>52</sup>

The United States has passed similar legislation to China and Russia in the shape of the CLOUD Act, which stipulates that government law enforcement agencies have the right to request the extraction of any data stored by American-based companies outside of the US, without requesting national authorities in those countries for aid<sup>53</sup>. This move has prompted the European Parliament to call for the suspension of the Privacy Shield, through which the US has given a political guarantee to restrict and limit government access to data held by certified companies<sup>54</sup>.

<sup>50</sup> Lee, Jyh-An, Hacking into China's Cybersecurity Law (May 7, 2018). Wake Forest Law Review, Vol. 53, 2018; The Chinese University of Hong Kong Faculty of Law Research Paper No. 2018-08. Available at SSRN: <https://ssrn.com/abstract=3174626> Accessed 21 October 2018

<sup>51</sup> <http://www.vietnam-briefing.com/news/vietnam-approves-new-law-cybersecurity.html> Accessed 21 October 2018

<sup>52</sup> <https://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data-localization-clarifications/> Accessed 21 October 2018

<sup>53</sup> <https://www.congress.gov/bill/115th-congress/house-bill/4943> Accessed 21 October 2018

<sup>54</sup> <http://www.europarl.europa.eu/news/en/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meeps> Accessed 21 October 2018



## 4.7 EU-GDPR – the new *de facto* global regulation?

Will GDPR become the new *de facto* global regulation? It will affect almost every company around the world that deals with the EU, and this may be a sign that GDPR will dominate the global scene, but it may not. National models for data protection can work well, and generally these follow some set of international framework or guidelines.

At the same time, GDPR remains open to sectoral co-regulation, such as the EU-US Privacy Shield, as a measure to ensure the legality of data transfers. The EU commission may decide that sectoral data protection legislation provides an adequate level of data protection, which means that national governments can choose to regulate certain sectors in a similar fashion to GDPR, without making such legislative initiatives economy wide, thus leaving room for divergence between countries, and securing the digital economy in crucial sectors.

It nonetheless remains to be seen how DPAs and industry regulators will view their roles going forward. As the different approaches from the FTC, the PDPC and the EU show, they can choose to facilitate or collaborate with industries and sectors in order ensure data protection and privacy. They can do this in the form of co-regulation, or by facilitating compliant self-regulation, or by issuing guidelines that are either company- or sector-based.

One way in which companies in third countries can show compliance is by adhering to codes of conduct which the EU Commission has approved on an EU-wide basis. It would be advantageous if such codes of conduct were not a purely European product, but were also facilitated in a more global setting. One such setting might be the Global Privacy Enforcement Network (GPEN), which consists of 53 privacy enforcement authorities in 39 jurisdictions (including the FTC, as well as European DPAs), with the purpose of promoting cooperation among privacy enforcement agencies<sup>55</sup>.

Even with all of these considerations, however, there can be no doubt that GDPR is set to have a tremendous impact on national data protection legislation outside of the EU. The newly proposed privacy bill in India is just one example of a third country adopting principles from GDPR<sup>56</sup>. New Zealand also passed new data protection legislation in 2017 which adopts many principles from GDPR, including data breach notifications and restrictions on cross-border data transfers, subject to the guarantee of appropriate safeguards<sup>57</sup>.

A globalized digital economy rightly needs more coordination and cooperation on privacy enforcement. The future of data privacy seems to require that regulators be involved in some way or other, whether through guidelines on self-regulation, or through co-regulatory measures.

<sup>55</sup> See Bennett, Colin, The Global Enforcement Privacy Network: A Growing Network But How Much Enforcement? (August 5, 2015). Available at SSRN: <https://ssrn.com/abstract=2640331> Accessed 21 October 2018

<sup>56</sup> <http://www.nishithdesai.com/information/news-storage/news-details/article/new-data-protection-law-proposed-in-india-flavors-of-gdpr.html> Accessed 21 October 2018

<sup>57</sup> <https://www.justice.govt.nz/assets/Documents/Publications/cabinet-paper-privacy-bill-2018-approval-for-introduction-and-additional-policy-decisions.pdf> Accessed 21 October 2018



## 5. A focus on digital identity within the framework protection of personal data

### 5.1 Digital identity

A digital identity is defined as ‘a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions’<sup>1</sup>. ITU defines it, in Recommendation ITU-T X.1252, as ‘a digital representation of the information known about a specific individual, group or organization’<sup>2</sup>.

While this description can be used to describe the use of email or other private services, this report uses the term to cover publically sanctioned or issued digital IDs with the same intended effects as official physical ID documents. This kind of e-ID can be used to prove your real-life identity online, and thereby grant access to a range of public and private services in a safe and secure way. With an e-ID, citizens are able not only to do their banking online, but also to gain access to crucial public services, including healthcare, pension, unemployment benefits and welfare – as well as in some cases allowing citizens to vote in national elections.

<sup>1</sup> <https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf> Accessed 21 October 2018

<sup>2</sup> See Recommendation ITU-T X.1252 *Baseline identity management terms and definitions*. Issues around the management of identity in data networks are further covered in Recommendation ITU-T X.1253 *Security guidelines for identity management systems*, and Recommendation ITU-T X.1254 *Entity authentication assurance framework*. See also ITU’s Digital Identity Roadmap Guide, 2018, available at: <https://www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx> Accessed 21 October 2018

E-ID is a two-way trust system. For providers of both public and private services, it gives the assurance that the person with the e-ID is who they claim to be. For people with e-ID, it gives them trust, both in the services they use, as well as in the e-ID itself having the required level of security, guaranteeing that only its owner can access and use it.

Trust in any e-ID system needs to be built around strong system security because of the higher risks involved with the services provided. There is a big difference between having credit card information stolen from a transaction online, and having a pension paid to a different person, or having full banking information delivered to a third party. If the e-ID is not properly secured, trust will very quickly erode between digital citizens and service providers. With digital identity, privacy, trust, and security are completely intertwined.

From a humanitarian, social and economic point of view, digital identities can help the nearly one billion people worldwide who lack any kind of ID, thereby allowing the delivery of services necessary for social inclusion as well as bringing them into the global economy<sup>3</sup>.

According to reports by ITU, the World Bank and GSMA, the creation of a digital identity goes through the following lifecycle:

#### *a) Registration*

This process involves collecting information that is unique to the person seeking digital ID. This can be biographical data (name, parents, gender, public identity number etc) as well as biometric data (fingerprints, iris scan, facial imaging etc). The data is then validated, including ensuring that the central database has no duplicate of the data registered for a different person. The type of data used during the registration process is key for the trustworthiness of the digital identity.

#### *b) Issuance of documents and credentials*

The digital identity can take many different forms. It can be issued as a smartcard, a sim card, or a mobile phone, for example, or it can exist entirely in the cloud.

#### *c) Authentication*

Authentication is one of the most important parts of any identity management system, allowing citizens to verify that the e-ID actually belongs to them. This can be achieved via biometrics, or via a two-factor authentication system; either way, authentication security is primordial.

## 5.2 Basic security

Digital identities are generally built on either Public Key Infrastructure (PKI) or Biometric verification.

PKI is asymmetric encryption. In a PKI system, there are two keys: a public key (with a personal certificate) and a private key. Any verified entity can have access to the public key, while the private key will only be known or accessible to the person holding the e-ID.

Messages encrypted by the public key can only be opened with the private key, and messages encrypted by the private key can only be opened with the public key. This means that as long as the private key is safe, the person using the public key can guarantee that the person on the other end is actually the verified person, and thereby send documents and messages that only the ID holder is able to open. This can be used to verify identity as strongly as any passport (because of the initial registration process and the trust in the safety of the private key), and is therefore sufficient to document and verify confidential online transactions, such as loan or welfare applications, for example. Private keys can be stored in special smart keys, USBs, sim cards, or in the cloud, which is then accessed online via a special login.

<sup>3</sup> See ITU, Digital Identity Roadmap Guide, 2018.

Biometric verification on the other hand, consists of a database on a server, which verifies the person's identity via biometric recognition. An individual's identity is confirmed by the match between biometric information, such as a physical fingerprint or iris scan, with the same information in the biometric database. Biometric verification can also be used at the device level, for example to access certain app functionalities; in this case, the data is stored on the device.

In order to ensure privacy and security, regulations on digital identity must also address technical and organizational requirements for the issuing of e-IDs. One example is the EU e-IDAs regulation, which ensures harmonized use of official, digital identities across all member states, and which sets specific requirements for security and authentication<sup>4</sup>.

### 5.3 Privacy considerations

From a privacy perspective, there are several things to be considered. One is the security aspect of a digital identity, which is described above. The other aspect is the actual creation of the digital identity itself, including access to and collection of the data during the registration phase, and the actual storage of biometric data, including storage security, and whether the central server confirmation has adequate security itself.

From a privacy perspective, biometric data is classified in Europe as sensitive data under GDPR, and thus has an extra layer of legislative protection. Unlike a PKI, which can be recalled, deleted, and replaced, biometric data is data relating directly to the physical characteristics of the person. While one can always verify one's identity by a simple fingerprint, one is also much more vulnerable if the database is compromised in terms of security, as it is not possible to simply get a new face or a new set of fingerprints.

### 5.4 Digital identity examples

#### A. Denmark

In Denmark, the digital identity system is based on PKI, and according to the administrative company concerned, it is based on a combination of consent and contractual agreement. The current service is called *NemID*, and the company behind it does not have the right to issue digital identities by itself. Instead, citizens have to apply for *NemID*, and the company will create a digital identity for them. Residents have to give consent for the collection of their personal identity number and they have full rights to withdraw the consent at any time – although if they do so, they will no longer have access to services requiring *NemID*<sup>5</sup>.

Rather than having a physical device with a public key, the key is stored centrally, and must be accessed via a special, secured connection, which includes password and two-factor identification in the form of a number from a physical (paper) key-card, a key generator, or via a mobile app.

As stated above, the security of the private key is the most important security aspect of any PKI system. The fact that the private key is stored on a server has led to criticism from the Danish DPA, who believes that the private key should physically be in the hands of the citizen, for example using a smart key. The central storage of private keys carries with it a high risk if the server is compromised, while a smart key gives citizens complete control over their private key<sup>6</sup>.

<sup>4</sup> Regulation (EU) No 910/2014: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN> Accessed 21 October 2018

<sup>5</sup> See *NemID* official webpage: [https://www.nemid.nu/dk-en/about\\_nemid/personal\\_data/](https://www.nemid.nu/dk-en/about_nemid/personal_data/) Accessed 21 October 2018

<sup>6</sup> <https://www.version2.dk/artikel/datatilsynet-er-forundrede-over-danids-forsinkede-private-noegle-33041> Accessed 21 October 2018

## B. Estonia

Estonia's digital identity system, *e-Estonia*, is similar to Denmark's, in using a PKI system for authentication in its digital identity solution, but instead of storing private keys on a central server, Estonia issues physical, private keys, which can be in the form of a sim card (Mobile-ID), or an ID card in the case of e-residency<sup>7</sup>. Mobile operators issue the digital identity (sim card).

Unlike Denmark, which created separate legislation, Estonia's e-identity is regulated in chapter 5 of the Estonian Identity Documents Act, thereby placing it legally in line with passports or other similar recognized physical documents, and requiring the same documentation for issuance<sup>8</sup>.

The Estonian system also uses a type of block chain technology, entitled KSI Blockchain, which validates each transaction done within the block, and signs off on it with a signature, adding it to the block, thereby guaranteeing the validity of transactions, and enabling an immutable workflow<sup>9</sup>.

## C. India

India's digital identity system, *Aadhaar*, started in 2009 with the aim of issuing digital identities to India's 1.2 billion citizens. The project is a venture between the Indian government, including the special authority, the Unique Identification Authority of India (UIDAI), and private companies, who have partly been charged with registration. More than one billion people are now enrolled in the system.

Biometric data is central to the functioning of *Aadhaar*. Rather than issuing a private key, people give their biometric data, and receive a paper with a Unique ID number in return. In order to verify their identity, they only need their number, and then the provider in question will validate the biometric data with the number via a request to a centralized server hosted by UIDAI. With *Aadhaar*, every Indian citizen has the possibility to access the services they need, and to become involved not just in society, but also in the digital economy.

## 5.5 Dynamic digital identities and cross-sectoral regulation

Another option could be the use of dynamic digital identities, which are identities based on captured behavioural history on multiple websites and apps. This allows for the verification of personal identity using personal characteristics such as typing style, movement of mouse pointer and perhaps even reading and time spent on websites. Such a system could verify, with a high degree of certainty, that people are who they say they are. However, from a privacy perspective, dynamic digital identities bear some risks of profiling and misuse if and when a person prefers not to be directly identified.

Regulators for their part need to be aware of the cross-sectoral aspects of the use of digital identities. If every website and any service can subscribe to the digital identity system, there is a risk of watering down the value of the identity, and this can lead to a higher incidence of identity fraud or identity theft. If even the simplest online shops and media sites require login with a digital identity, users would quickly become accustomed to giving away their details, and may inadvertently deliver it to phishing sites, which could then use it to access personal bank accounts, or to redirect public services.

In order to have a properly functioning digital identity, there needs to be a certain restriction on the types and numbers of services which require the use of digital identity for authentication.

<sup>7</sup> For sim card, see: <https://www.id.ee/index.php?id=36881>, e-residency: <https://e-resident.gov.ee/become-an-e-resident/> Both accessed 21 October 2018

<sup>8</sup> <https://www.riigiteataja.ee/en/eli/528032017002/consolide> Accessed 21 October 2018

<sup>9</sup> See whitepaper by Guardtime: <https://m.guardtime.com/files/Guardtime-whitepaper-Volta.pdf>, and <https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf> Both accessed 21 October 2018



## 6. Data security

With personal data, when examining the issues of trust and security, it is important to remember that data is, at all times, owned by the data subject and that data has a value. It may be ‘leased’ to organizations, but the owner is ultimately the person who the data refers to<sup>1</sup>. As with more traditional valuable assets, data is also subject to theft or malicious damage – and the more often the general public sees data breaches, the less inclined they will be to share personal data (a ‘tipping point’ was discussed earlier). With personal data being the lifeblood of the digital economy, its free flow is built on consent, and trust is crucial<sup>2</sup>.

As an example of how regulation can define security objectives, GDPR sets out its expectations concerning organizations’ handling of the personal data of EU citizens, wherever they are in the world:

There are a number of areas to be examined when looking at data security, since this is fundamental in building consumer trust in organizations processing and storing personal data. Data is vulnerable, both when at rest and in transit. The risk to organizations will also vary depending on the data’s value – both to organizations, in terms of the business value, or the impact of a breach on the business, and to the data subjects themselves.

For example, it could be argued that the loss of a list of a thousand patients’ medical records would pose a much larger risk than the loss of a list of a thousand IP addresses. This is also due to the value that adversaries may place on the data. Medical information can often contain a large amount of personal data, including social security numbers, names, addresses, and biometric data. Understanding this risk is crucial; too much or too little security applied to securing data will either overburden organizations and risk extinguishing growth in the digital economy, or will introduce unnecessary risk.

<sup>1</sup> This is subject to a number of exceptions, however, depending on national and regulatory caveats.

<sup>2</sup> ITU-T developed the 305x and 125x series of Recommendations dealing with trust and personal data protection. As explained in module 4 of ITU’s ‘AI for Development’ series, Recommendation ITU-T Y.3052 provides an overview of trust provisioning in ICT infrastructures and services. Recommendation ITU-T Y.3052 introduces necessity of trust to cope with potential risks due to lack of trust. The concept of trust provisioning is explained in the context of trusted ICT infrastructures and services.

*'In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage<sup>1</sup>.'*

<sup>1</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

The most obvious technical control to safeguard data however is to ensure that it is always encrypted – both when stored and when in transit. However, if the solution were that simple, and it is that easy to secure data, then why are we seeing the highest levels of data breaches ever recorded?

## 6.1 What barriers does industry face in securing data?

Securing data is easy – but it can be difficult to secure data that you can access and process easily, share safely, and update when required, all while keeping costs down.

The following five barriers contribute to preventing the safe storage, processing and transmission of data:

### *Awareness of the data landscape*

Many organizations are finding that they do not fully understand their data landscape. The increased use of vendor cloud services, as well as the rise in remote and collaborative working, means that data can be stored across multiple devices, multiple locations and multiple organizations, including any third parties. Organizations that do not understand the edges of their data landscapes may well be inadvertently growing their attack surfaces.

### *Awareness of threat landscape*

Companies seeking to exploit commercial opportunities in the digital economy must keep a close eye on the data they collect, store and share with third parties, in order to know what they need to defend.

*'According to Risk Based Security's 2017 Data Breach QuickView report, there were 5,207 breaches recorded in 2017, surpassing 2015's high mark by nearly 20%. The number of records compromised also surpassed all other years, with over 7.8 billion records exposed, a 24.2% increase over 2016's previous high of 6.3 billion<sup>1</sup>.'*

<sup>1</sup> <https://www.infosecurity-magazine.com/news/2017-worst-year-ever-for-data-loss> Accessed 22 October 2018.

Organizations need to increase awareness of the threats they face as guardians of data. To give just one example, data controllers and processors in the healthcare industry are now well aware of the significant risks associated with holding large amounts of personal data, following the data breach

at Anthem in early 2015, which saw 78.8 million patient records stolen. The attack harvested highly sensitive data, including names, Social Security numbers, home addresses, and dates of birth<sup>3</sup>.

### *Appetite*

Another significant barrier is appetite. One of the dangers of introducing stringent data protection regulations is that it can slow the growth of the digital economy by simply proving too difficult for non-data protection specialists to implement. Organizations may choose to take the risk of a lower level of data protection than may be necessary, believing that the risks are not high, or that the costs of compliance are higher than the costs of potential data breaches.

### *Cost*

The fourth barrier is the cost of increased data protection activities. In a similar vein to appetite, above, implementing technical solutions to secure data is not cheap, and it may be that an organization's business model has to adapt to the fact that data protection is now an added financial overhead.

Any new entrant to the digital economy faces considerable costs simply launching their product or service, and being noticed amongst all the 'digital noise' can add significant costs. If implementing safe data control security measures is too expensive when the company starts operating, it may spend years playing catch up, leaving significant vulnerabilities open.

It is therefore crucial that regulators provide clear, effective guidance on how organizations can secure data while minimizing the implementation costs where possible. A great example of this is the British National Cyber Security Centre's guidance series on topics such as GDPR compliance and cybersecurity for small businesses<sup>4</sup>.

### *Ability*

The final barrier is ability. The coming into force of new regulations is generally welcomed by consumers, but it can pose real problems for those who must adhere to them. Indeed, when GDPR came into force, many firms struggled to define the outcomes they actually needed to achieve in order to be compliant<sup>5</sup>. Clear regulation, with defined outcomes and actionable steps to be taken should help to minimize the burden on organizations, allowing their data protection activities to flourish and adding value to the business model.

## 6.2 Regulators

Data protection regulation is not new, but the need for it is growing rapidly, particularly in the light of significant data breaches which affect ever-larger numbers of consumers. Data subjects now expect that their data be held in a secure, transparent manner, and for consumer protection to be in place.

Regulators are now taking a leading role in defining standards and reasonable expectations for organizations and companies, and the steps they must take in order to safeguard personal data. Nonetheless, applying a blunt solution to a complex and very variable data landscape can lead to rather vague standards. In GDPR's sections on security, for example, there is only rather generic advice, which can lead to organizations' inability to implement, as mentioned earlier:

<sup>3</sup> <https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time> Accessed 22 October 2018.

<sup>4</sup> <https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes> Accessed 22 October 2018.

<sup>5</sup> <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-deloitte-gdpr-benchmarking-survey.pdf> Accessed 22 October 2018.



*‘Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects<sup>1</sup>.’*

<sup>1</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Adding to the problem of ambiguous definitions is the issue of how security regulation is delivered. As seen in chapter 4, there are a number of models, ranging from direct government regulation to self-regulation. Co-regulation offers a flexible middle way approach to defining and attaining standards. This allows industry and government to combine and incorporate industry established standards for cybersecurity containing measures for data protection.

Organizations and companies can choose to either comply with ISO 27001, or become externally certified, demonstrating their commitment to their customers to data security. With ISO 27001 controls that would require implementation to be compliant or certified can be scaled, depending on the size and complexity of the organization. This scalable model makes for easier co-regulation definition and measurement, and delivers a layered approach to data protection security.

### 6.3 Manufacturers

Traditionally, security vendors have based their products and technology on traditional security practices such as creating a secure perimeter – on the premise that if you build a wall high enough and put all your assets behind it, you should be reasonably safe. While this may have worked in the past, as data increasingly becomes the product, and the sharing of it becomes essential to commercial success, this approach causes problems, including the lower availability of information and a dangerously false perception of safety.

There are a number of newer technologies and concepts now available to security practitioners. These include:

*Secure boot* – Many vendors now offer secure boot processes on their hardware, and some operating systems, including Windows 10, offer Secure Boot options<sup>6</sup>. The new Unified Extensible Firmware Interface (UEFI) essentially starts encryption and integrity checks from the chip level upwards.

*Patching* – While the responsibility to patch systems is a responsibility for organizations, vendors themselves are now investing more time and money in finding vulnerabilities in their products, and releasing patches to mitigate these more quickly than ever before.

*Encryption* – There is now much more encryption build in and implemented across systems, including built-in disk encryption, Hypertext Transfer Protocol Secure (HTTPS) websites, and Trusted Platform Module (TPM) chips, which safely hold encryption keys.

*Authentication* – It is becoming increasingly rare to be able to access sensitive data such as online banking or social media without having to go through some sort of two-factor authentication (2FA).

<sup>6</sup> <https://www.csoonline.com/article/3107984/data-protection/6-security-advances-worth-celebrating.html> Accessed 22 October 2018

The biggest development in security, however, is blockchain, which has been described as a disruptor to the way many industries process database-based transactions. Much in the same way that some of the two-sided market companies such as Uber have disrupted traditional taxi companies, blockchain is set to do the same in industries from banking to healthcare.

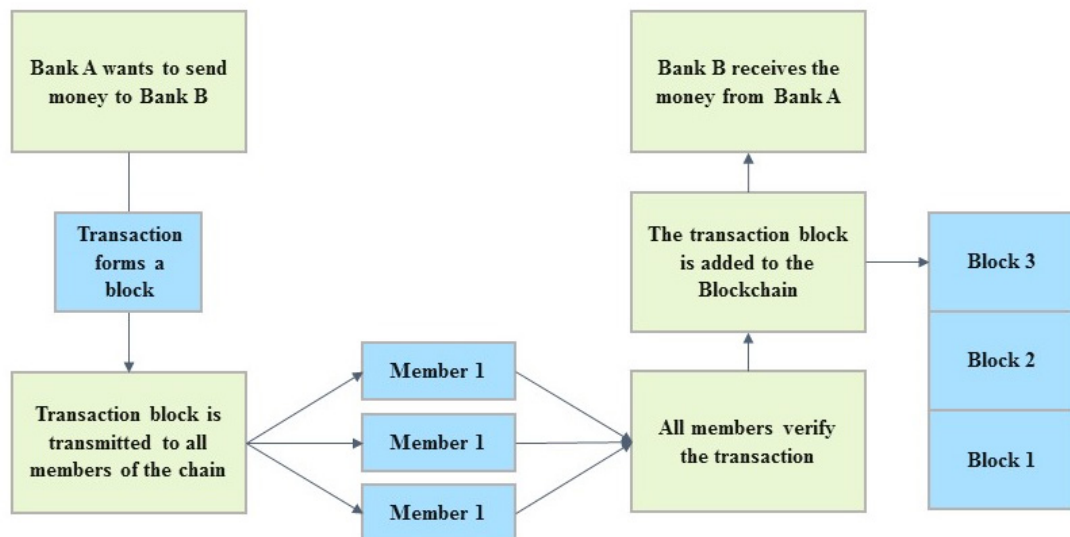
The potential value of the global blockchain technology market is estimated to be worth up to USD 20 billion by the end of 2024<sup>7</sup>, while Gartner suggests that blockchain’s business value-add will grow to USD 176 billion by 2025<sup>8</sup>.

The significance of the development of blockchain is what it offers in terms of security to data protection. Firstly, Blockchain is decentralized, so it does away with the traditional idea of a central data storage solution and instead spreads the storage of data across those using that particular blockchain.

A simple way to explain it (without going into technical detail) is to use the analogy of two banks transferring money from one account to another. Traditionally, the banks hold their own records of what money they hold. From a security point of view, this provides a single point of failure and a single, defined target. As one bank transfers money to another, there is a check that the money has been received and updates are sent to two different data records. With blockchain, the records the banks hold are identical, and they are updated together, almost instantaneously, vastly improving efficiency and security.

Blockchain can deliver more efficiency to transactions, more security through distribution and higher levels of integrity through peer approval, and there will be many opportunities for using it to power the digital economy. It is important to note however that blockchain is not a two-sided economy application, or a business model in itself; it is a technology that can be applied to and used by platforms that make up the business model of the two-sided economy.

Figure 8 – Blockchain



<sup>7</sup> <https://www.prnewswire.com/news-releases/blockchain-technology-market-to-gain-revenue-worth-us20-bn-by-2024---tmr-686428221.html> Accessed 22 October 2018

<sup>8</sup> <https://www.gartner.com/doc/3776763/things-cios-need-know-blockchain> Accessed 22 October 2018

## 6.4 Distributed ownership, distributed risk

How would this apply in practice? Much in the same way as the bank example shown above, transactions taking place online and the sharing of data could both be done using blockchain technology. Once implemented into markets, the technology would provide a next-generation level of security for personal data. Hackers can currently infiltrate networks with relative ease and go to servers or storage devices and remove or change data. They would struggle to do this against the multiple targets they would need in a distributed blockchain model, however, as they would effectively have to target all members of the blockchain at the same time. This is currently beyond the vast majority of hackers.

Blockchain offers a significant leap forward in terms of data security, but ensuring that the infrastructure supporting it is also secure – as well as the people using it, which is always the greatest vulnerability – is another area that requires work in parallel.

Blockchain would also offer a much higher level of protection to the integrity of data, since any data changed in only one part of the blockchain would be much quicker to spot than in traditional storage solutions.

The technology community is clearly increasingly enthusiastic about advances in digital security technology, but the most important audience, those consenting to the use of their data, may need more convincing. Raising the level of public trust in security technologies could be a successful motivator in letting an increasingly sceptical public hand over control of their data. For this to be the case, however, complex technological practices need to be translated into simple, publicly consumable communication materials. Complementing the technology itself, it will also be critical to deliver accompanying improvements in employee understanding of their data protection responsibilities. For every reported data breach (each of which can affect millions of data subjects) what is the corresponding positive narrative which can help raise public confidence. And, crucially, who owns that responsibility?



## 7. Conclusion

In this report, it has been demonstrated how privacy, security and trust work together to power and fuel the digital economy and help create innovations across the ICT sector. At every step of the value chain, across sectors, privacy and security need to be adopted, and worked into the entire process.

Companies who rely on data will have to comply with new legislative models which are being implemented around the world, and in particular with the extraterritorial effects of EU GDPR.

This clearly creates challenges for both companies and regulators, going forward. How do you translate general principles of data protection into concrete actions, which the ICT industry must follow? Companies face many challenges in determining adequate levels of security, and implementing privacy considerations, and some will be liable to forego the whole assessment altogether.

This is one point where regulators can step in and assist, by facilitating compliant self-regulation, or co-regulatory measures in individual companies, or even across entire sectors. Whichever models are chosen, a fully-powered global digital economy will concerted efforts to harmonize privacy and security.

At the same time, advances in technology create new areas of possibility, as well as new legal and regulatory challenges. Blockchain technology in particular appears to hold great promise for the future. Digital identities, whether public or private, also hold the potential for stimulating the global digital economy by bringing more citizens into the fold, and building trust across services, as well as between the private and public actors.

As a new dawn begins for privacy and security regulations, one thing remains certain: the challenges are global, and every country has a stake.

**International Telecommunication Union (ITU)**  
**Telecommunication Development Bureau (BDT)**  
**Office of the Director**  
Place des Nations  
CH-1211 Geneva 20 – Switzerland  
Email: [bdtdirector@itu.int](mailto:bdtdirector@itu.int)  
Tel.: +41 22 730 5035/5435  
Fax: +41 22 730 5484

**Deputy to the Director and  
Director, Administration and  
Operations Coordination  
Department (DDR)**  
Email: [bdtddeputydir@itu.int](mailto:bdtddeputydir@itu.int)  
Tel.: +41 22 730 5784  
Fax: +41 22 730 5484

**Infrastructure Enabling  
Environment and  
e-Applications Department (IEE)**  
Email: [bdtiee@itu.int](mailto:bdtiee@itu.int)  
Tel.: +41 22 730 5421  
Fax: +41 22 730 5484

**Innovation and Partnership  
Department (IP)**  
Email: [bdtip@itu.int](mailto:bdtip@itu.int)  
Tel.: +41 22 730 5900  
Fax: +41 22 730 5484

**Project Support and Knowledge  
Management Department (PKM)**  
Email: [bdtpkm@itu.int](mailto:bdtpkm@itu.int)  
Tel.: +41 22 730 5447  
Fax: +41 22 730 5484

## Africa

**Ethiopia**  
**International Telecommunication  
Union (ITU)**  
**Regional Office**  
P.O. Box 60 005  
Gambia Rd., Leghar ETC Building  
3rd floor  
Addis Ababa – Ethiopia

Email: [itu-addis@itu.int](mailto:itu-addis@itu.int)  
Tel.: +251 11 551 4977  
Tel.: +251 11 551 4855  
Tel.: +251 11 551 8328  
Fax: +251 11 551 7299

**Cameroon**  
**Union internationale des  
télécommunications (UIT)**  
**Bureau de zone**  
Immeuble CAMPOST, 3<sup>e</sup> étage  
Boulevard du 20 mai  
Boîte postale 11017  
Yaoundé – Cameroun

Email: [itu-yaounde@itu.int](mailto:itu-yaounde@itu.int)  
Tel.: +237 22 22 9292  
Tel.: +237 22 22 9291  
Fax: +237 22 22 9297

**Senegal**  
**Union internationale des  
télécommunications (UIT)**  
**Bureau de zone**  
19, Rue Parchappe x Amadou  
Assane Ndoye  
Immeuble Fayçal, 4<sup>e</sup> étage  
B.P. 50202 Dakar RP  
Dakar – Sénégal

Email: [itu-dakar@itu.int](mailto:itu-dakar@itu.int)  
Tel.: +221 33 849 7720  
Fax: +221 33 822 8013

**Zimbabwe**  
**International Telecommunication  
Union (ITU)**  
**Area Office**  
TelOne Centre for Learning  
Corner Samora Machel and  
Hampton Road  
P.O. Box BE 792 Belvedere  
Harare – Zimbabwe

Email: [itu-harare@itu.int](mailto:itu-harare@itu.int)  
Tel.: +263 4 77 5939  
Tel.: +263 4 77 5941  
Fax: +263 4 77 1257

## Americas

**Brazil**  
**União Internacional de  
Telecomunicações (UIT)**  
**Regional Office**  
SAUS Quadra 06, Bloco “E”  
11<sup>o</sup> andar, Ala Sul  
Ed. Luis Eduardo Magalhães (Anatel)  
70070-940 Brasília, DF – Brazil

Email: [itubrasilia@itu.int](mailto:itubrasilia@itu.int)  
Tel.: +55 61 2312 2730-1  
Tel.: +55 61 2312 2733-5  
Fax: +55 61 2312 2738

**Barbados**  
**International Telecommunication  
Union (ITU)**  
**Area Office**  
United Nations House  
Marine Gardens  
Hastings, Christ Church  
P.O. Box 1047  
Bridgetown – Barbados

Email: [itubridgetown@itu.int](mailto:itubridgetown@itu.int)  
Tel.: +1 246 431 0343/4  
Fax: +1 246 437 7403

**Chile**  
**Unión Internacional de  
Telecomunicaciones (UIT)**  
Oficina de Representación de Área  
Merced 753, Piso 4  
Casilla 50484, Plaza de Armas  
Santiago de Chile – Chile

Email: [itusantiago@itu.int](mailto:itusantiago@itu.int)  
Tel.: +56 2 632 6134/6147  
Fax: +56 2 632 6154

**Honduras**  
**Unión Internacional de  
Telecomunicaciones (UIT)**  
Oficina de Representación de Área  
Colonia Palmira, Avenida Brasil  
Ed. COMTELCA/UIT, 4.º piso  
P.O. Box 976  
Tegucigalpa – Honduras

Email: [itutegucigalpa@itu.int](mailto:itutegucigalpa@itu.int)  
Tel.: +504 22 201 074  
Fax: +504 22 201 075

## Arab States

**Egypt**  
**International Telecommunication  
Union (ITU)**  
**Regional Office**  
Smart Village, Building B 147, 3rd floor  
Km 28 Cairo – Alexandria Desert Road  
Giza Governorate  
Cairo – Egypt

Email: [itucairo@itu.int](mailto:itucairo@itu.int)  
Tel.: +202 3537 1777  
Fax: +202 3537 1888

## Asia and the Pacific

**Thailand**  
**International Telecommunication  
Union (ITU)**  
**Regional Office**  
Thailand Post Training Center, 5th  
floor,  
111 Chaengwattana Road, Laksi  
Bangkok 10210 – Thailand

Mailing address  
P.O. Box 178, Laksi Post Office  
Laksi, Bangkok 10210 – Thailand

Email: [itubangkok@itu.int](mailto:itubangkok@itu.int)  
Tel.: +66 2 575 0055  
Fax: +66 2 575 3507

**Indonesia**  
**International Telecommunication  
Union (ITU)**  
**Area Office**  
Sapta Pesona Building, 13th floor  
Jl. Merdan Merdeka Barat No. 17  
Jakarta 10001 – Indonesia

Mailing address:  
c/o UNDP – P.O. Box 2338  
Jakarta 10001 – Indonesia

Email: [itujakarta@itu.int](mailto:itujakarta@itu.int)  
Tel.: +62 21 381 3572  
Tel.: +62 21 380 2322  
Tel.: +62 21 380 2324  
Fax: +62 21 389 05521

## CIS countries

**Russian Federation**  
**International Telecommunication  
Union (ITU)**  
**Regional Office**  
4, Building 1  
Sergiy Radonezhsky Str.  
Moscow 105120  
Russian Federation

Mailing address:  
P.O. Box 25 – Moscow 105120  
Russian Federation

Email: [itumoskow@itu.int](mailto:itumoskow@itu.int)  
Tel.: +7 495 926 6070  
Fax: +7 495 926 6073

## Europe

**Switzerland**  
**International Telecommunication  
Union (ITU)**  
**Telecommunication Development  
Bureau (BDT)**  
**Europe Unit (EUR)**  
Place des Nations  
CH-1211 Geneva 20 – Switzerland  
Switzerland  
Email: [eurregion@itu.int](mailto:eurregion@itu.int)  
Tel.: +41 22 730 5111

International Telecommunication Union  
Telecommunication Development Bureau  
Place des Nations  
CH-1211 Geneva 20  
Switzerland

ISBN: 978-92-61-28151-9



Published in Switzerland  
Geneva, 2018