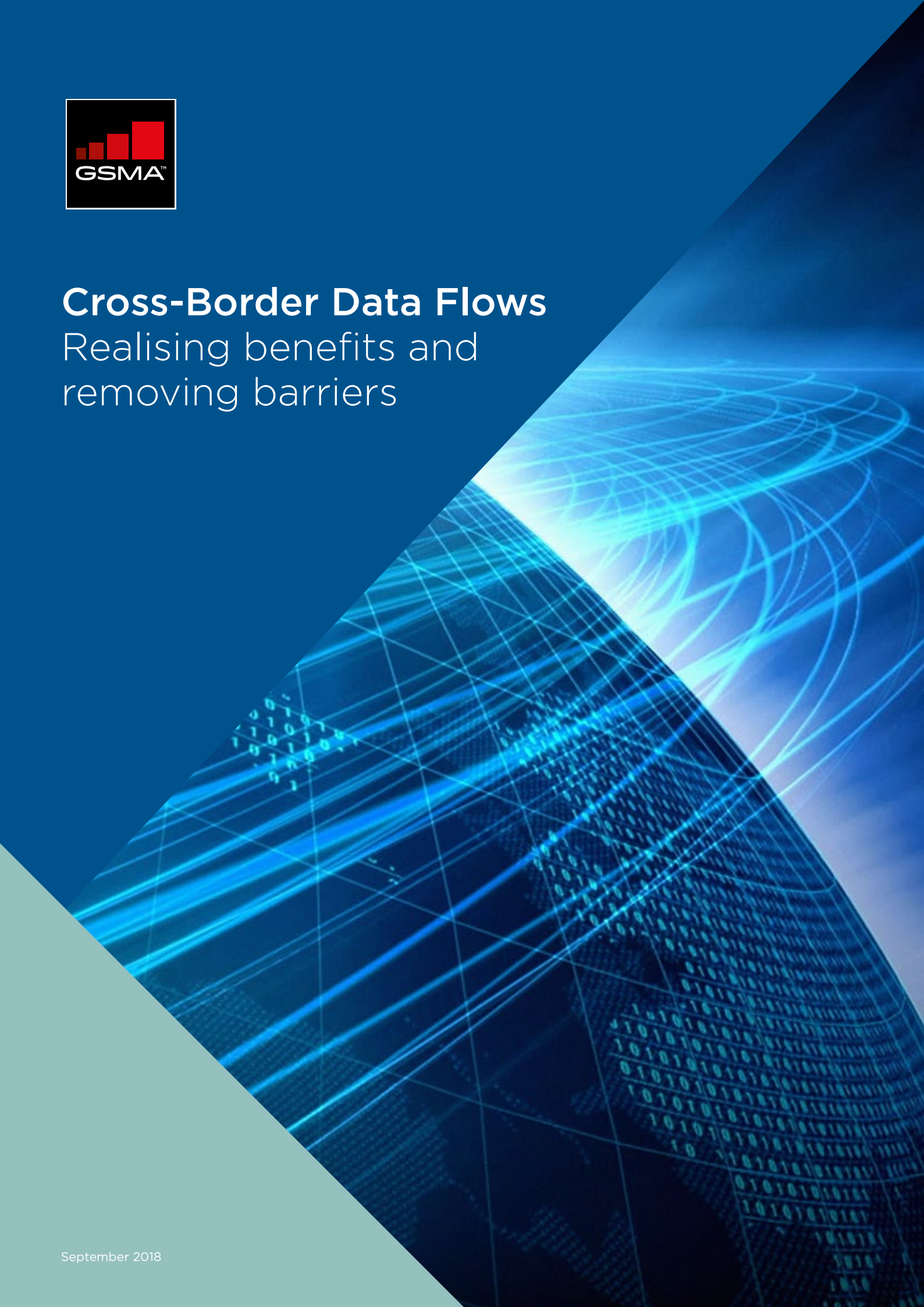
Cross-Border Data Flows

Realising benefits and removing barriers



September 2018

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com and public policy website at www.gsma.com/publicpolicy

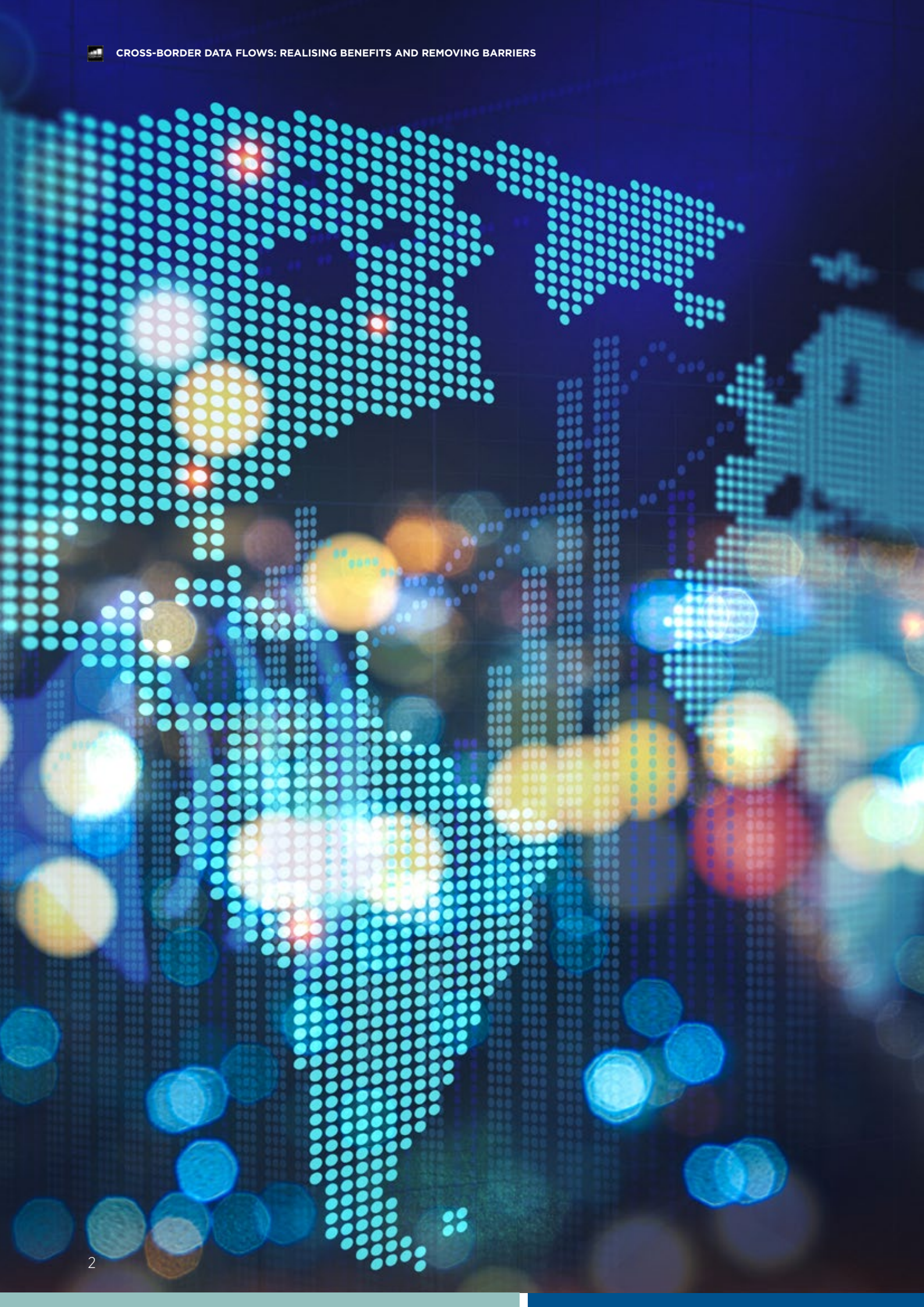
To view the GSMA's related resources online, visit www.gsma.com/CrossBorderDataFlows

Follow the GSMA on Twitter: @GSMA and @GSMAPolicy

Authors

The GSMA commissioned Wickham Heath Consulting to conduct research and write this report. Wickham Heath Consulting Limited is a UK-based consultancy dealing primarily with the regulation of new communications and Internet Platform products.

CONTENTS



Summary

Today's commerce relies on organisations' ability to move data – including consumers' personal data – across borders without restriction. The ability to do so generates positive outcomes not only for organisations, but for citizens and countries as well.

Any organisation, no matter how small, can use the internet to market and deliver its ideas, goods and services, wherever data is allowed to flow. Cross-border data transfers enable digital goods and services to be accessed more or less instantly and physical goods to be ordered for delivery, regardless of where the items are produced. Organisations respond to consumer demand by expanding to serve more geographic markets, leading to more consumer choice. At the same time, companies that operate in multiple countries gain efficiencies by centralising and virtualising their data analysis, processing and storage.

A number of countries have introduced restrictions on the flow of data across borders, stemming from national security concerns, data privacy concerns or the desire to protect domestic markets. These restrictions take different forms, such as obtaining explicit consent from citizens or prior authorisation from data protection authorities. More prohibitive rules prevent organisations from transferring any personal data or metadata at all.

The effects of such restrictions are many. For instance, requiring organisations to hold an additional copy of data generated from their activities in a country increases the costs of producing physical and digital goods and services in that market. Costs are increased further when the analysis and processing of data must be conducted domestically in addition to storage.

Like other international businesses, telecoms operators want to realise the efficiencies of centralisation and virtualisation. However, the metadata they generate about individuals' communications is often subject to sector-specific, pre-digital regulations or licence obligations that prohibit the movement of metadata out of that country and instead mandate its collection and storage. Such telecoms-specific restrictions put telecoms operators at a disadvantage compared to unregulated providers of communications services such as internet platforms.

In response to the rising incidence of data localisation measures around the world, this paper presents a number of recommendations for governments to unlock the benefits of cross-border data flows for individuals, organisations, governments and the economy, while ensuring sufficient data privacy rules are in place to protect citizens and maintain their trust in the digital ecosystem.

Recommendation 1:	Commit to facilitating cross-border data flows and removing unnecessary localisation measures
Recommendation 2:	Ensure privacy frameworks are fit for a digital age
Recommendation 3:	Review legacy sector-specific privacy rules
Recommendation 4:	Encourage regional data privacy initiatives
Recommendation 5:	Avoid localisation by addressing foreign surveillance concerns pragmatically
Recommendation 6:	Avoid localisation by addressing law enforcement and national security concerns pragmatically

Introduction: Understanding the benefits of freely flowing data

Data is fundamental to today's digital and physical commerce and it is a vital catalyst for innovation. Development of the digital economy and continued productivity growth in traditional industries depend on organisations' ability to transfer data, including consumers' personal data, within and between countries for efficient analysis, processing and storage. The freedom to move personal data without restriction between countries generates positive outcomes not only for organisations, but for citizens and countries as well.

Benefits to citizens

For individuals, internet access provides the means to interact with people and organisations anywhere in the world – whether local, domestic, in a neighbouring country or on another continent.

International data flows support access to the wide range of goods and services available online. Digital goods and services can be accessed more or less instantly, and physical goods can be ordered for delivery, regardless of where the items are produced.

Organisations respond to consumer demand by expanding to serve more geographic markets, giving those customers access to a wider range of goods and services. Overall, this expansion of digital and physical marketing increases customer choice and satisfaction. The free movement of data across borders enables organisations to use common infrastructure to serve multiple markets, so digital goods and services spread to customers more rapidly. This particularly benefits small and medium-size enterprises that do not have an international footprint.

Scenario 1[1] describes one individual's use of the internet – which is reliant on international data transfers – to widen her life chances, develop herself professionally and pursue business opportunities.

1. The scenarios in this paper are fictional and intended to illustrate the benefits of cross-border data flows and the disadvantages of restricting data flows. They are based on and inspired by discussions with telecoms operators and industry representatives about real experiences; they should not be regarded as real-world cases.

Scenario 1: **International data transfers enable individual opportunity**

Luisa learns to cook while growing up in Spain. As an adult, she moves to another country and continues to cook, keeping up to date with new recipes from her native region using the internet. Her digital identity and preferences improve her internet experience and facilitate the discovery of information about Spanish regional food, including recipes and cooking videos.

She sets up a successful mobile pop-up business cooking Spanish regional food at parties and events. Luisa subsequently opens a cookery school, offering adult evening and day cookery classes in her home, and later is able to open a small restaurant. To create distinctive food, she continues to use the internet, email and electronic money transfer to order ingredients from specialised wholesalers, including some in Spain, who deliver internationally. Over time, the business expands into larger premises and employs more people.

Luisa's success in creating a small-scale enterprise depends on internet access and the movement of data across borders. As she has gradually expanded her professional activities to create employment for herself and others, the government has benefitted through taxation. And many customers enjoy her regional Spanish food.

Benefits to countries and society

Permitting data to be exchanged across borders can bring more national businesses and consumers into the digital fold, encouraging the adoption of data-driven business strategies and stimulating the national economy.

Internet service growth at a national level is supported by flexible approaches to the transfer of data across borders. The free movement of personal data delivers social and economic benefits more rapidly than the alternative, which would require businesses to structure their back-office, processing and storage functions to serve multiple individual markets.

The strategic role of the transfer of data across borders has been recognised by policymakers:

- The Council of Europe[2] explains that: *"global information flows play an increasingly significant role in modern society, enabling the exercise of fundamental rights and freedoms while triggering innovation and fostering social and economic progress, while also playing a vital role in ensuring public safety."*

- APEC[3] recognises: *"the importance of the development of effective privacy protections that avoid barriers to information flows and ensure continued trade and economic growth in the APEC region. […] Regulatory systems that unnecessarily restrict this flow or place burdens on it have adverse implications for global business, economies and individuals. Therefore, in promoting and enforcing ethical information practices, there is also a need to develop systems for protecting privacy that account for these realities in the global environment."*

- UNCTAD[4] quotes research by the McKinsey Global Institute: *"The international dimension of flows [of goods, services and finance has] increased global GDP by approximately 10 percent, equivalent to a value of $7.8 trillion in 2014. Data flows represent an estimated $2.8 trillion of this added value."*

- The OECD[5] states that: *"Cross-border data flows have increased economic efficiency and productivity, raising welfare and standards of living."*

- The European Commission[6] argues that: *"Unjustified restrictions on the free movement of data are likely to constrain the development of the EU data economy […] risk fragmenting the market, reducing the quality of service for users and reducing the competitiveness of the data service providers, especially smaller entities."*

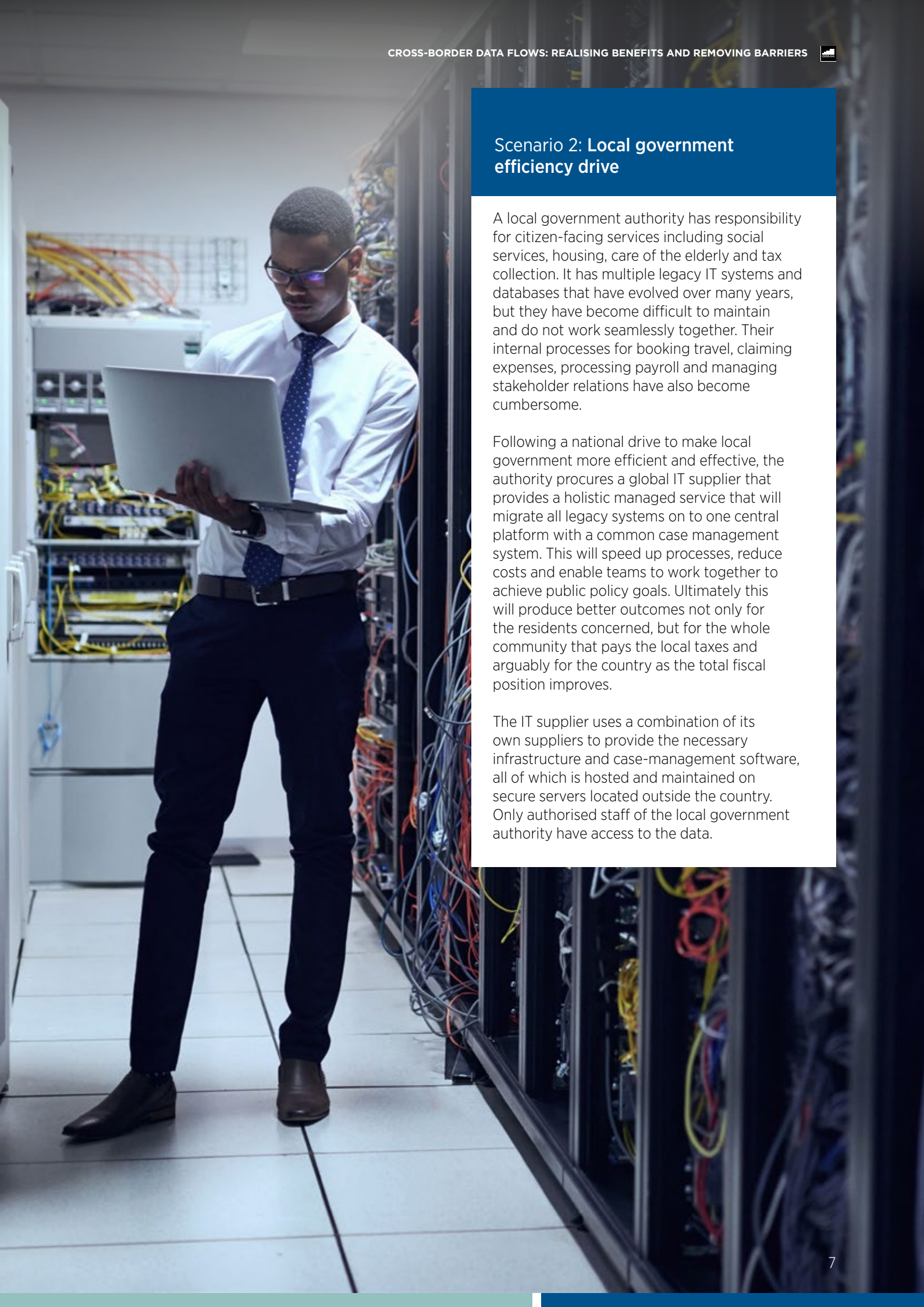
- The International Chamber of Commerce (ICC)[7] urges governments *"to ensure all citizens and companies can realise the full potential of the Internet […] by adopting policies that facilitate the adoption of new technologies and global movement of data that supports them."*

- Addressing the role of cross-border data flows in the manufacturing sector, the National Board of Trade in Sweden[8] argues: *"A constant and seamless flow of goods, services, capital, people, and data is necessary for competitive production. […] the movement of data already is an indispensable part of today's production process [and] will be even more central to production in the future."*

Regulatory regimes that facilitate the international transfer of data allow small, specialised organisations to establish an internet presence that is simultaneously national and international. Services can emerge and be successfully adopted in one national market, then expand to other markets, bringing rapid benefits for second and subsequent countries.

Public-sector bodies and government departments also benefit from cross-border data flows allowing them to deliver better quality public services at a lower cost and pursue public policy objectives that might not otherwise be achievable, as the following two scenarios illustrate.

2. Council of Europe, Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, (CETS 223), 2018. Para 12.
3. Asia-Pacific Economic Cooperation, Updates to the APEC Privacy Framework, 2016/CSOM/012app17.
4. United Nations Conference on Trade and Development (UNCTAD), Data protection regulations and international data flows: Implications for trade and development, 2016.
5. OECD, 2012 Internet Economy. Paper 143.
6. European Commission, Building a European Data Economy, COM (2017) 9 final.
7. ICC, Trade in the digital economy – A primer on global data flows for policymakers, 2016.
8. National Board of Trade (Sweden), No Transfer, No Production – A Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods, 2015.



Scenario 2: **Local government efficiency drive**

A local government authority has responsibility for citizen-facing services including social services, housing, care of the elderly and tax collection. It has multiple legacy IT systems and databases that have evolved over many years, but they have become difficult to maintain and do not work seamlessly together. Their internal processes for booking travel, claiming expenses, processing payroll and managing stakeholder relations have also become cumbersome.

Following a national drive to make local government more efficient and effective, the authority procures a global IT supplier that provides a holistic managed service that will migrate all legacy systems on to one central platform with a common case management system. This will speed up processes, reduce costs and enable teams to work together to achieve public policy goals. Ultimately this will produce better outcomes not only for the residents concerned, but for the whole community that pays the local taxes and arguably for the country as the total fiscal position improves.

The IT supplier uses a combination of its own suppliers to provide the necessary infrastructure and case-management software, all of which is hosted and maintained on secure servers located outside the country. Only authorised staff of the local government authority have access to the data.

Scenario 3: **Big Data for Social Good**

The mayor of a capital city has set ambitious goals for reducing pollution. Her team commissions a project that combines data from weather stations, fixed air quality sensors and telecoms operators. The anonymised and aggregated data from the telecoms operators provides detailed insights into the travel patterns of commuters and visitors on an ongoing basis. This enables the city to incentivise travel at other times or by other means of transport, and allows for a more granular and cost-effective monitoring of pollution in the city compared with a static sensor network collecting equivalent data.

To get even better results, the project intends to collaborate with other cities around the world to compare the severity of pollution levels between cities and discover patterns and insights about which policy decisions are most effective. This will benefit all participating cities, their inhabitants and visitors.

In order to collaborate effectively, the participating cities and companies sign an agreement and jointly appoint a leading analytics provider that hosts the anonymised and aggregated data on a common platform. Although the analytics is conducted across all the contributed data sets, no city or company has access to any of the raw data contributed by another party. However, they all benefit from the actionable insights generated. As a result, the mayor achieves her ambitious targets, and people gain improved daily quality of life and better long-term health outcomes.

Benefits to organisations

Any organisation, no matter how small, can use the internet to market and deliver its ideas, goods and services, wherever data is allowed to flow. This would not be possible without data moving between countries, so organisations can provide information and products in response to individuals' requests.

Cross-border data flows also allow multinational organisations to become more efficient by centralising and virtualising their internal operations. These organisations are able to expand their business cost-effectively, using flexible, cloud-based infrastructure and specialist application service providers and minimising investment in additional IT equipment.

International businesses of all types are adopting data-driven digital transformation strategies to secure their future. This may involve internal process reform or external IT and business outsourcing. These competitive strategies depend on being able to collect, analyse, process and store data across multi-country operations. Where data can flow, new forms of data analytics become possible, allowing organisations to generate insights into the views of their customers and the performance of their operations and products.

Allowing free movement of personal data internationally permits businesses to improve service quality and reduce costs and, under competition, this leads to lower customer prices. Internet infrastructure suppliers, cloud computing providers and telecoms operators can structure their services to cater to large numbers of customers in multiple markets at the lowest overall cost.

For example, Scenario 4 describes a major Asian telecoms operator that is using cross-border data transfers to improve its mobile network service quality and demonstrates how this benefits customers and governments.

Scenario 4: **Centralisation and virtualisation of data enhances mobile network service quality**

A major Asian telecommunications operator improves its network service quality by creating a single centre to provide enhanced network management and quality assurance for its national operating businesses. The new, group-wide centre monitors network performance, congestion and fault occurrences. This virtual capability allows the operator to access and compare data on performance and fault conditions across its footprint, which would be impossible with national-level network management only.

The new centre has access to more sophisticated network and service management tools from equipment suppliers and is able to use a single supplier's monitoring and diagnostic tools across multiple national markets. This has improved mobile network quality while optimising investment. By forming a 'centre of excellence' to enhance its network and service management, the operator has been able to develop national employees' technical capabilities through secondments from national operating businesses and other career development activities.

Analysing data collected from national markets means the operator can proactively diagnose fault conditions, including more complex network faults, while spreading its capital and staffing costs across all customers in its footprint. For consumers and national governments, mobile voice, data and internet service quality are improved by data centralisation.

Governments can help to achieve all of the above benefits through public policy frameworks that facilitate cross-border data flows to the maximum extent possible, while also accomplishing other public policy objectives such as data privacy and security.

Restrictions on cross-border data flows

Reasons given for imposing restrictions

A number of countries have introduced restrictions on the cross-border flow of data. Reasons for introducing restrictions differ from country to country, but typically include one or more of the following justifications:

- **Data privacy and security.** Data may be processed in countries that do not have equivalent privacy regulation in place and could be more vulnerable to hacking.
- **Foreign surveillance.** Data held internationally may be vulnerable to surveillance by the foreign government or others.
- **National security.** Internet platform companies and telecoms operators that hold data internationally may not be compelled to provide the same support to law enforcement or national security organisations.
- **National digital economy.** Encouragement of in-country data analysis, processing and storage may be perceived as a way to protect or stimulate the national digital economy.

Types of restrictions

For organisations, the impact of restrictions on cross-border data flows varies, depending on the nature of the restriction applied. Types of restrictions include:

- **Conditional data flows** – Where data privacy and security are the basis for the restriction, organisations may be required to seek prior authorisation from regulators including data protection authorities, obtain consent from citizens or enter into prescribed contractual clauses with each downstream recipient of the data. Frameworks that enable general permissions such as APEC's Cross-Border Privacy Rules and the EU's Binding Corporate Rules can be more attractive as they allow organisations to transfer data within a corporate group or to specific recipients on an ongoing basis. However, the processes to obtain such permissions can be burdensome and costly. Where one country considers another country to have a privacy regime that provides an 'adequate level of protection' or is 'equivalent' to its own, data may be transferred freely between the countries. However, such 'adequacy' findings take a long time to be completed and apply to very few countries.
- **Localisation + subsequent flows** – Organisations may be obligated to keep a copy of all personal data and metadata in the home country, while additional copies of the data may be transferred abroad for centralised analysis, processing and storage.
- **Localisation** – Organisations may be subject to more prohibitive rules that stop them from transferring personal data or metadata altogether.

These may be the result of historic obligations in licences or other permissions required by telecoms operators or other providers, or of newer regulation which may now be applied to any company active in the provision of digital services.

- **Indirect** – Indirect (and in some cases unwritten) rules may have the effect of keeping data in a specific country or requiring it to be held by a national supplier.

Impact of restrictions

Where additional safeguards, such as standard contractual clauses or consent, are required in relation to each transfer of personal data, this can represent a significant administrative burden for organisations. It can also result in the safeguard being perceived as a mere administrative exercise with little real benefit for data subjects. Mechanisms are much more effective when they encourage organisations to put in place holistic programmes to protect personal data wherever it may be processed. Such mechanisms grant organisations general permissions to move data across borders while allowing organisations to focus on the identification and mitigation of risk.

Requiring organisations to hold an additional copy of data generated from their activities in a country increases the costs of producing goods and services in that market. Companies must commission and operate national-scale data centres which might otherwise support multiple national markets or even be supplied globally from one or (to increase resilience) two data centres.

Costs are increased further when the analysis and processing of data must be conducted domestically in addition to storage. In this case, the regulation requires organisations, in effect, to supply digital goods and services using duplicate, national-scale businesses located in individual regulated national markets. Depending on companies' systems architecture and technical implementation, this more onerous type of regime delays and fragments the introduction of digital goods and services and reduces their viability.

As examples, see Scenario 5 that discusses remote fault detection by a vehicle manufacturer, and Scenario 6 which details the international deployment of an Internet of Things (IoT) service by an international telecoms operator.

Scenario 5: **Automobile fault-detection across borders**

Modern vehicles are increasingly intelligent, equipped with devices to capture data on engine performance and to detect vehicle faults. Mechanics can query this data to diagnose faults more efficiently. Some manufacturers use machine-to-machine (M2M) technology to link fault-monitoring data to central servers, enabling the detection and diagnosis of a fault before it becomes evident to the car owner. M2M is also used to alert customers of the need for vehicle servicing. Cross-border data flows feature strongly in these reliability-enhancing and potentially life-saving scenarios, as automobiles and commercial vehicles cross borders all the time.

To take the benefits even further, connected cars enable the use of big data analytics by manufacturers, revealing performance characteristics of an entire line of connected vehicles. This scenario only applies, however, in markets or jurisdictions where manufacturers are permitted to connect to customers' vehicles and analyse the data collected. Countries that do not permit consumer data to flow freely across borders will, as a result, inhibit remote vehicle diagnostics and thus the realisation of safer, more reliable transport.

Scenario 6: **Multinational IoT service relies on single data centre**

An international telecommunications operator has developed a service that allows consumers, using a mobile application, to locate, monitor and track items such as family cars, rucksacks, pets or livestock. Through this service, the real-time condition of items can be checked, lost items can be found and alarms can be set based on an item's location.

The service is launched internationally using a common data centre, so each national market can be served without replicating computer systems for each market. Manufacturers can also experiment with their products to discover what customers in different national markets and segments find valuable.

In markets that require a localised, in-country data centre, the service provider faces higher costs to customise and deploy the product architecture. It therefore decides to forgo launching the service in these markets at this time. The consequence of cross-border data flow restrictions is that customers are denied access to low-cost tracking and monitoring of personal items; manufacturers cannot test products to see their value in their national market; and governments miss the economic and tax benefits of this innovative and useful service.

It should be noted that the manner in which such localisation restrictions are implemented or interpreted by national authorities can significantly mitigate the negative impact that they may otherwise have. Where governments insist on passing such measures, they should, therefore, engage with industry and other stakeholders before the measure is implemented.

Examples of national restrictions

Certain markets have substantially diverged, or are now considering diverging, from a model supporting the free flow of data across borders.

Within the category of restrictions based on data privacy concerns, the extent to which personal data can flow varies. South Korea, for example, imposes strict consent requirements for transfers of personal data with very limited exceptions such as the data transfer being mandated by law, necessary to perform a public function or necessary to protect vital interests in an emergency. Côte d'Ivoire only allows personal data transfers based on prior authorisation or to countries that have an adequate level of protection, but it is not clear which countries are considered to have this. Other countries provide organisations with a more flexible array of exceptions and transfer mechanisms to choose from which significantly reduces the impact of the restriction.

The restrictions that cause the biggest difficulties for organisations are the ones that require, directly or indirectly, data to be kept within the country. Russia, for example, requires organisations (including subsidiaries of foreign companies) that collect the personal data of its citizens through electronic communications to store this data nationally.[9] Personal data must be placed in a primary database located and maintained in Russia. Although data may subsequently be transferred abroad and placed in secondary databases, provided other legal requirements[10] for the treatment of such data are complied with, the requirement to keep the original data in Russia necessitates additional resources.

Telecoms operators, internet platform companies and others in Indonesia that provide a 'public service' to Indonesian customers through an electronic system are required to establish a national data centre and disaster recovery centre.[11] This includes

9. Federal Law of 21 July 2014 No. 242-FZ amended certain legislative acts of the Russian Federation in relation to personal data processing information and telecommunications networks.
10. Including the Personal Data Law of 27 July 2006 N 152-FZ which prohibits the cross-border transfer of data to countries that do not provide adequate protection of data subjects.
11. Regulation No. 20 of 1 December 2016 on Personal Data Protection in Electronic Systems which implements Government Regulation 82 of 2012: Regarding the Provision of Electronic Systems and Transactions.

services provided by non-governmental institutions in banking, communications, health, insurance, industrial services, security and social networking sectors. The justifications given for establishing both a national data centre and a disaster recovery centre have been for the purposes of law enforcement and data protection. Cross-border data transfers are permitted, in principle, subject to the agreement of the Indonesian Ministry of Communications and Informatics, although this process is subject to further clarification.

The Pakistan Telecommunications Authority and State Bank of Pakistan prohibit telecoms and financial companies from transferring customer data overseas. However, other data, including email content, can be legally transmitted and stored outside the country. Similar licence conditions apply in India.

In Vietnam, the existing requirement to store data on local servers has recently been replaced by a requirement for offshore telecoms and internet service providers with more than 10,000 users to have headquarters or representative offices in Vietnam and store personal data of users from Vietnam within the country.

In Germany, telecoms operators are obliged to retain traffic and location data within Germany (although this is not currently enforced due to multiple legal challenges). Kazakhstan is considering a law that would oblige telecoms operators to store subscriber data only in Kazakhstan apart from when it is necessary for roaming purposes.

Responses to national privacy concerns

Where the declared rationale for restricting cross-border data flows is data protection, policymakers argue that personal data may not be protected when transferred internationally, and individuals may not have sufficient rights in countries that do not have the same safeguards.

This concern is valid, but a proportionate and effective response should be a national or regional framework for data privacy, which protects citizens and consumers nationally while providing suitable international data transfer mechanisms with associated safeguards.

Where privacy concerns relate to information security, this is arguably based on a misconception that data stored in a specific national market is more secure than data stored internationally. However, effective information security cannot be distilled into a single element, such as where data happens to be physically stored. It depends on a broad combination of factors, including storage infrastructure, the intelligence of security protocols, use of encryption and other IT best practice.

Mandating national data storage creates friction with data security, as it requires separate investment for individual markets, on a national scale. This is more expensive and more vulnerable to intrusion than larger-scale, international corporate defences.[12]

Many countries and regions are now adopting regulatory models to ensure data can flow across borders, while being subject to appropriate data protection requirements.

Data privacy is regulated at different levels in the United States. Some federal laws target particular sectors or activities such as fair credit reporting or use of health data while state laws range from security breach reporting to more comprehensive laws. At the federal level, the Federal Trade Commission enforces good data privacy practices through its jurisdiction over unfair and deceptive business acts and practices and in relation to some specific matters such as children's privacy. The Federal Communications Commission sets rules for and supervises network providers. Generally speaking, these laws do not restrict the movement of data out of the US, but focus instead on holding organisations accountable for any use of the data by the organisations or their suppliers. The US engages positively with regional frameworks to facilitate cross-border data flows, participating in the APEC CBPR system and the EU-US Privacy Shield. The US approach, focused on accountability, has permitted the national digital goods and services businesses to grow rapidly and, it may be argued, to dominate much of the international economy in digital goods and services.

12. Amazon Data Residency Whitepaper February 2018 provides an extended discussion of security from the perspective of a *'hyper-scale'* cloud service provider at: https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

The European Union adopted the influential Data Protection Directive[13] in 1995. This approach has evolved into the General Data Protection Regulation[14] (GDPR). The GDPR is intended to provide consistent EU-wide protection of personal data, while permitting it to flow within the EU and to third countries which are deemed to have 'adequate' data protection regimes. Under the GDPR, organisations that can demonstrate to data protection authorities that they handle personal data responsibly, either through so-called 'binding corporate rules' or through certifications, can benefit from general permissions to transfer personal data out of the EU. The law also offers a range of other mechanisms and exceptions[15] to provide organisations with a degree of flexibility to address their data flow needs in a way that suits their organisation best. Recent proposals in several countries around the world have started to follow the GDPR model. In Brazil, for example, transfers of personal data will be allowed under the new law provided the third country has adequate mechanisms to protect personal data and facilitate institutional and judicial cooperation.

In September 2017, the European Commission published a further proposal designed to ensure free flow of 'non-personal' data to enhance the European digital economy. This measure proposes:

- The free movement of non-personal data within the EU (to complement that of personal data);
- Public authority access to data located in another EU Member State or in the cloud; and
- A self-regulatory approach to switching between cloud service providers for professional users.

How the measure to regulate non-personal data will operate is not yet clear. However, the European Commission argues that securing free movement of data within the EU will support the European digital economy and generate an additional 0.7% GDP by 2020, up from 0.2% in 2013.[16]

Countries in the Asia-Pacific region have developed a common model of international data flow regulation under the auspices of APEC, whose Cross-Border Privacy Rules (CBPR) stipulate how data flows between APEC economies should operate.

There are three major elements of APEC CBPR:

- Adoption of shared principles in the treatment of personal data;
- Creation of enforcement mechanisms where data is transferred between member economies; and
- Accountability of organisations that must be able to demonstrate that they have certain safeguards in place before they are granted a general permission to transfer data.

Currently there are six participating economies: the US, Mexico, Japan, Canada, Singapore, and the Republic of Korea, with others actively looking to join in the near future.

Japan's Act on the Protection of Personal Information was initially passed in 2003, subject to amendment in 2015 with final entry into effect on 30 May 2017. In addition to establishing a fully-functional independent data protection authority, the amendment sought to facilitate cross-border data flows through the provision of a range of mechanisms, recognising the importance of data flows to the digital economy. These purposely include the possibility for organisations to demonstrate responsible data governance through certification under CBPR.

Recent discussions between Japan and the EU led to the European Commission's announcement in July 2018 that they will formally recognise each other's data protection systems as providing an equivalent level of protection for consumers in both markets. This will create the world's largest area – encompassing 37 per cent of global trade by value – within which personal data can flow freely while receiving a consistent level of protection. The EU and Japan expect to ratify the process of finding each other's data protection systems as 'adequate' before the end of 2018. Japan is now well placed to support the free flow of international data both across Asia-Pacific and with the EU, albeit under different privacy frameworks.

Countries that adopt internationally accepted data protection approaches benefit economically from shared digital services infrastructure operating at a global scale. Such 'data-connected' markets form an internationally integrated data flow mainstream, where digital goods and services can be produced at global scale and quality.

13. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
14. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR was agreed in 2016 and applied to organisations processing data from 25 May 2018.
15. For more information on the range of transfer mechanisms typically made available, please see CIPL paper: Cross-Border Data Transfer Mechanisms, August 2015.
16. "SMART 2013/0043 - Uptake of cloud in Europe" study by IDC on Quantitative estimates of the demand for cloud computing in Europe and likely barriers to take-up. Quoted in Measuring the economic impact of cloud computing in Europe by Deloitte which is, in turn, quoted by the EC in support of its proposed Directive.

Responses to foreign surveillance and national security concerns

Information disclosed by Edward Snowden in 2013 regarding the activities of the US National Security Agency (NSA) exposed the existence of agreements with a number of internet platform companies to gain access to the private data of non-US nationals. Unsurprisingly, the revelation of extensive, secret NSA surveillance of private digital service data located in the US troubled governments internationally. This gave impetus to concerns about the foreign surveillance of data held in other national markets.

In the five years following Snowden's disclosure, a partial response to these concerns has been the diversification of countries in which internet platform companies and cloud computing providers operate data centres or regional hubs. This allows organisations and governments that are concerned about foreign surveillance activities to avoid data being held in particular jurisdictions. However, allowing organisations this level of geographic control inevitably comes at a cost which must either be absorbed by the business customer or ultimately the downstream consumer.

In addition, cloud computing providers are able to offer customers, such as telecoms operators, the ability to securely encrypt digital data – where the keys for such data may be held nationally and so be resistant to decryption. Other techniques, such as anonymisation and aggregation, may also be used to prevent the identification of personal data transmitted internationally. These developments, together, substantially mitigate risks of foreign surveillance where data is held internationally.

In contrast to steps that address foreign surveillance concerns, progress on addressing countries' law enforcement and national security concerns has not been as pronounced. It is understandable that governments are concerned about losing access to data that may be useful to their law enforcement authorities, but which is processed and controlled by internet companies based outside of their countries.

Existing multilateral provisions for the sharing of data in support of law enforcement can be used, but these have been argued to operate slowly and imperfectly.

In the face of these imperfections, law enforcement and national security interests have argued for national data storage and/or service operation because this provides a control point over the activities of internet platform companies and telecoms operators. A number of governments have gone further by limiting the activities of internet platform companies where they have been found to be uncooperative with national law enforcement or to undermine national security.

However, recent developments in this regard include the US CLOUD Act, the EU eEvidence proposal and additional protocol to the Budapest Convention on Cybercrime. These initiatives offer hope that new ways will be found to provide clear and predictable frameworks that give organisations legal certainty and give authorities more direct and timely access to the offshore data they need, thereby removing the need for localisation measures.

To address foreign surveillance and law enforcement concerns requires pragmatism both on the part of countries and companies. Ultimately, countries that turn their backs on services available in the global digital economy must fall back on national-scale production of goods and services. For their part, major commercial players in a national market will find it difficult to ensure a sustainable business if their operations are seen to undermine law enforcement or national security.

Responses to concerns for the national digital economy

The regulation of cross-border data flows may also be perceived by some as a way to protect the economic interests of nations and their businesses. Yet this notion has significant flaws. In particular, requiring national data processing and storage or national digital service production:

- Restricts these activities to the relevant national scale of operation, and this is likely to lead to significantly higher costs of operation per customer served;
- Embeds other national production factors into digital services (e.g., if a country is subject to electricity supply constraints, these can be overcome in part through the use of international data storage and digital service production);
- Is likely to delay, limit or even prevent citizens' access to innovative digital services that emerge on the global stage; and
- Fails to acknowledge the value to the national economy of skills and insights that are only available if data can flow across borders.

Once again, an aligned and coordinated policy approach that removes restrictions and liberates the flow of data will deliver benefits for national markets.

For example, Scenario 7 illustrates how restrictions on cross-border data flows affect not just digital product development, but also the efficiency of traditional manufacturing.

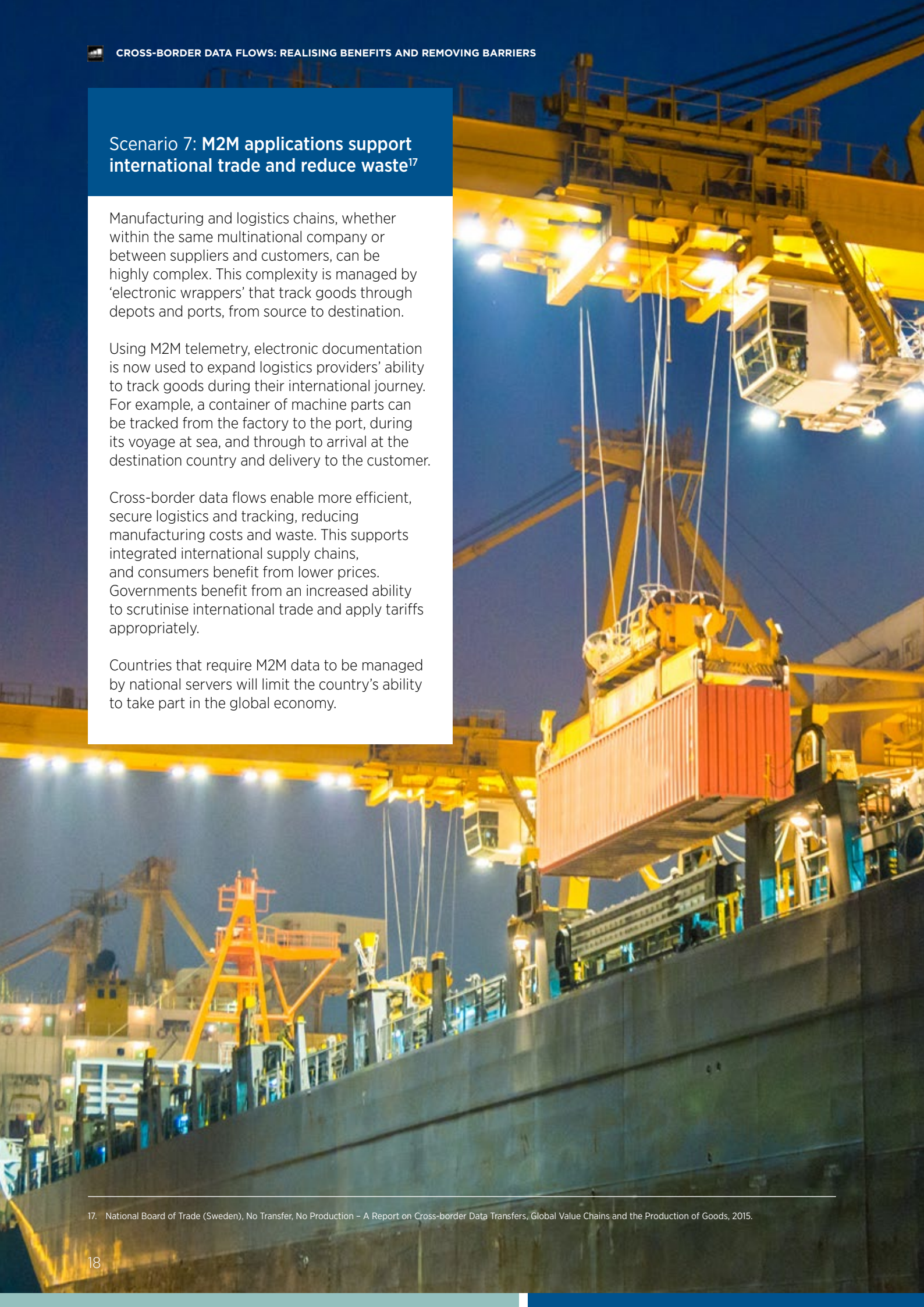
Scenario 7: **M2M applications support international trade and reduce waste**[17]

Manufacturing and logistics chains, whether within the same multinational company or between suppliers and customers, can be highly complex. This complexity is managed by 'electronic wrappers' that track goods through depots and ports, from source to destination.

Using M2M telemetry, electronic documentation is now used to expand logistics providers' ability to track goods during their international journey. For example, a container of machine parts can be tracked from the factory to the port, during its voyage at sea, and through to arrival at the destination country and delivery to the customer.

Cross-border data flows enable more efficient, secure logistics and tracking, reducing manufacturing costs and waste. This supports integrated international supply chains, and consumers benefit from lower prices. Governments benefit from an increased ability to scrutinise international trade and apply tariffs appropriately.

Countries that require M2M data to be managed by national servers will limit the country's ability to take part in the global economy.



17. National Board of Trade (Sweden), No Transfer, No Production – A Report on Cross-border Data Transfers, Global Value Chains and the Production of Goods, 2015.

In the absence of shared regional approaches, national restrictions to the free flow of data on the part of certain markets seem likely to create two divergent tracks of digital market development:

- **Data-connected markets,** including most developed and many emerging markets where digital goods and services are cheap to produce and are offered to citizens and customers at global scale and quality.

- **National-scale digital markets**, subject to restrictions on the cross-border movement of data and thus limiting supplier opportunities and consumer economic benefit.

Given current policy divergences, it seems likely that data-connected markets will have the advantage as locations for production and consumption, and will progressively expand their share of international digital and physical trade over time.

Policymakers considering the alternative national-scale digital market model should consider carefully the economic consequences of separating analysis, processing and storage in their country from the internationally integrated data-flow mainstream. This approach risks leaving their countries in a national cul-de-sac that will limit digital growth in their market, in comparison to international competitors.


57.1713
11.7157
96.5843
17.9512
26.5584
98.0398
44.3256
40.7901

Impact of cross-border data restrictions on the telecoms sector

The core purpose of telecoms operators is to connect people regardless of location and distance. While telecommunications started with telegrams and progressed to voice calls, SMS and emails, it now involves the exchange of data at scale and operators' infrastructure and services carry this data.

Telecoms operators share a common goal with other international businesses: they want data to flow so they can realise the efficiencies of centralisation and virtualisation. However, because they have traditionally been national players with physical infrastructure in a country, the metadata they generate about individuals' communications – who they connect with, from where and for how long – is often subject to sector-specific, pre-digital regulations or licence obligations that prohibit the movement of metadata out of that country and instead mandate its collection and storage.

Such telecoms-specific restrictions act as a barrier to achieving the sort of efficiency that has become the norm for most other international businesses and puts telecoms operators at a disadvantage compared to unregulated providers of communications services such as internet platforms.

Telecoms operators are also at the forefront of the emerging Internet of Things and are supporting advances in automation from remote weather sensors to connected cars. To enable these technologies and unlock their potential benefit, operators need common business models and technologies that will work anywhere in the world. If telecoms operators are burdened with legacy telecoms-specific restrictions on cross-border data flows, they will be placed at a disadvantage in comparison with internet platforms, and the development of these technologies and business models will be much slower and more expensive.

To the extent that telecoms-specific restrictions are founded on the perceived sensitivity of metadata and the need to protect the privacy of the individuals concerned, this paper argues that it is more effective to protect individuals' privacy through horizontal, risk-based data protection mechanisms. Rather than being a separate category of data that is always deemed to be sensitive, the sensitivity of metadata depends on the context in which it is processed and the safeguards applied in each case. Horizontal data privacy laws that apply to the processing of all personal data provide sufficient protection by placing duties on organisations to identify and mitigate risks of harm to individuals. Where data is moved abroad, these safeguards can be made to apply by extension without disrupting the flow of data.

Telecoms-specific restrictions are also imposed in order to enable law enforcement authorities and intelligence services to gain lawful and appropriate access to data. Historically, telecoms operators were natural targets for this type of requirement given that they already had physical infrastructure and data processing centres in each country and that, before the arrival of the internet, their metadata was one of the best and most obvious sources of intelligence. However, it should also be recognised that the telecoms industry is under pressure to take advantage of cloud-based infrastructure and software services in the same way that other sectors have done. As well as being efficient and good for consumers, using cloud-based services means that there is no operational need to conduct certain processing activities within physical proximity to the communications hardware within a country.

Concerns from law enforcement authorities that they will no longer be able to access data they need for investigations are legitimate. However, rather than forcing local collection and storage of all data or forcing telecoms operators to provide access to all internet traffic that passes over their networks, governments should, in the future, look to policy initiatives such as the US CLOUD Act and the EU eEvidence proposal to address these concerns.

In the meantime, it is also incumbent on telecoms operators that are starting to centralise and virtualise their operations to provide pragmatic reassurance to national authorities that they will continue to support their legitimate law enforcement requests.

Improved approaches to facilitating cross-border data flows

The mobile industry believes that cross-border data flows are essential to unlock benefits for individuals, organisations, governments and the economy both nationally and internationally. To identify the benefits of free movement of data is not to suggest that there should be no regulation in this area. A shared view by many policymakers, organisations and civil society is that smart data privacy regulation can both enable data flows and protect citizens, providing consumers and policymakers with confidence in digital goods and services.

In order to enable the benefits highlighted in this paper, the GSMA would encourage governments to act on the following recommendations:

Recommendation 1: Commit to facilitating cross-border data flows and removing unnecessary localisation measures

Governments should make a firm commitment to facilitating cross-border data flows and removing unnecessary localisation measures in order to realise the benefits of the free movement of data for individuals, businesses and governments.

Public commitment, whether at a national level or within the context of a regional or multilateral body, can set a clear direction and strategic vision to stimulate the digital economy nationally and encourage alignment across the region. Where localisation measures do go ahead, governments should consult with stakeholders regarding how the measures will be interpreted and implemented.

Recommendation 2: Ensure privacy frameworks are fit for a digital age

Policymakers should ensure that legal frameworks effectively address data protection concerns in their country. Such frameworks should describe citizens' and consumers' privacy rights and the obligations on organisations when collecting, analysing, processing and storing data.

In order to be fit for a digital age, national privacy frameworks should be based on "the core set of data protection principles that are said to be at the heart of most national [privacy] laws and international regimes".[18] Such approaches should reflect consumer concerns over data privacy and security[19] and should operate on a technology and sector-neutral basis so customers are assured of consistent treatment of their data. They should also provide for the creation and resourcing of a national data protection authority.

Privacy regulation should focus on risks of harm to individuals and incorporate measures to ensure accountability on the part of organisations collecting data, while providing for flexible implementation to allow organisations to innovate rapidly, achieve larger scale and reduce their costs of production.

18. UNCTAD, Data protection regulations and international data flows: Implications for trade and development, 2016. See: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
19. See, for example, privacy research published by the GSMA in 2014: https://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf

Recommendation 3: Review legacy sector-specific privacy rules

Historically, operators have often been the subject of sector-specific restrictions on international data flows. The core purpose of telecoms operators is connecting people regardless of location and distance. While telecommunications started with telegrams and progressed to voice calls, SMS and emails, it now involves the exchange of data at scale, and operators' infrastructure and services carry this data. With data being a driving force in the digital economy, it no longer makes sense to treat telecoms operator data differently from data generated by other providers of electronic communications or indeed by the wider digital economy. Enacting a national privacy framework that is fit for a digital age provides an opportunity for a review of legacy sector-specific rules on privacy to ensure they are still required.

Recommendation 4: Encourage regional data privacy initiatives

Supranational bodies including APEC and the European Union have already adopted regulatory models for data protection and privacy while ensuring that data can flow freely across the region. These models provide a proportionate and effective response for policymakers who wish to protect citizens and consumers while also supporting future international trade in physical and digital goods and services.

Regional data privacy initiatives should be encouraged and implemented on the basis of common principles, should support interregional data flows, and should be interoperable with existing APEC and EU approaches[20] and with similar national approaches. Regional initiatives build regulatory capacity in data privacy and the development of industry best practice for the treatment of data. This will build confidence between countries, facilitate sharing of best practice between policymakers and allow data privacy regulators to detect and address non-compliance more easily.

Addressing national consumer privacy and security concerns consistently by region will facilitate cross-border data flows while providing data governance mechanisms to ensure industry accountability nationally and internationally.

Recommendation 5: Avoid localisation by addressing foreign surveillance concerns pragmatically

Governments should consider the range of options available to protect data that is deemed sensitive, rather than mandating its localisation. These options include encryption, anonymisation and aggregation, and, in certain circumstances, may include the specification of particular regional hubs for specific types of data.

Recommendation 6: Avoid localisation by addressing law enforcement and national security concerns pragmatically

Governments should engage with initiatives such as the additional protocol to the Budapest Convention on Cybercrime, the US CLOUD Act and the EU eEvidence proposal to provide clear and predictable frameworks that give organisations legal certainty and give authorities more direct and timely access to the offshore data they need, thereby removing the need for localisation measures.

Adopting these recommendations will:

- Enable the digital economy to operate efficiently and deliver social and economic benefits more rapidly in multiple nations and regions;
- Provide people with access to a global range and high quality of services, overcoming national market constraints where they exist; and
- Permit established businesses, including telecoms operators, to adopt data-driven digital transformation strategies to reduce costs and consequently the prices for digital and physical goods in the marketplace.

20. In particular, be interoperable with APEC Cross-Border Privacy Rules (CBPRs), EU Binding Corporate Rules (BCRs) and the associated common reference model established by a joint APEC / EU working party.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London, EC4N 8AF,
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601