INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

ICC WHITE PAPER ON
Trusted Government Access to Personal Data Held by the Private Sector

CONTENTS

INTRODUCTION

The essential role of global data flows in today's economy became evident when the pandemic lockdown started in 2020, and companies of all sizes around the world responded by transitioning their businesses to online-first or online-only, and their operations to remote work. Cross-border data flows are at the heart of the world's economy, as companies rely on such flows to conduct their day-to-day business with customers and partners, innovate in their business and operations, and compete more effectively, in sectors as diverse as agriculture, healthcare, manufacturing and banking.[1]

These data flows underpin every aspect of today's business—cloud services, customer relationship management, human resource management, remote work, workplace collaboration, and supply chain management. They also underlie distance learning, telemedicine, the fight against cybercrime and child abuse online, fraud monitoring and prevention, investigation of counterfeit products, and a broad range of other activities. Retailers send data across borders when they check inventory in an overseas warehouse, accept and process customer orders, and enable customers to track shipments enroute to their destination. Global companies of all sizes across industries rely on cloud-based human resources systems to hire employees and conduct performance reviews, and to administer benefits and payroll across offices in different countries. In particular,

1 Testimony of Victoria A. Espinel, President and CEO, BSA | The Software Alliance, Before the U.S. Senate Committee on Commerce, Science and Transportation, *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows* (December 9, 2020).

small- and medium-sized enterprises (SMEs) leverage cloud services to reduce barriers of entry to markets, enabling them to be on equal footing with much larger and/or better resourced organisations at lowered costs. Data flows help these organisations to do market research, extend their market reach, access latest innovations, and collaborate with other organisations to minimise economic and technical uncertainties.[2] International collaborations on COVD-19 research and responses rely on such flows to enable new understandings of the virus, tracking of the spread of the pandemic and evolution of the variants, and development and distribution of vaccine.

The processing and transfer of personal data are integral to many of these exchanges, making trust a vital element for resilient and sustainable economic growth and recovery. However, trust in international data flows is being eroded over concerns that government demands to access data may conflict with universal human rights and freedoms, including privacy rights, or cause concerns and conflicts with domestic laws when such access transcends borders. These increased concerns and reduced trust have led to uncertainty that may discourage individuals,' businesses,' and even governments' participation in a global economy, and can negatively impact inclusive and resilient economic growth. This lack of trust can lead to disruption in global data flows and thus business operations, products and service. It can also serve as the rationale for an increasing number of compelled data localisation measures globally.

Governments have legitimate interests in preventing, investigating and prosecuting serious crime, as well as in addressing national security threats. Addressing the trust deficit require governments to enact robust and comprehensive national privacy regulations, with firm commitments to protecting the rights and freedoms of individuals, including the fundamental right to privacy, when personal data is subject to government access.

The lack of clarity, transparency, and consistency between national approaches to government access to data has led to a steady growth in the number and restrictiveness of measures to constrain cross-border data flows. Moreover, inconsistencies in the implementation of law enforcement and national security interests in national laws, and the lack of international norms and interoperability of policy and regulatory regimes have created significant administrative burdens on businesses, while eroding the trust of businesses, people, as well as governments in using digital technologies, and impacting their potential in the digital economy.

With 60% of global GDP digitised by 2022, and growth in every industry driven by data flows and digital technology,[3] disruptions in cross-border data flows will have broad reverberations that can lead to reduced potential GDP gains and adverse impact on the local/national digital ecosystems—at a time when economic recovery is top of agenda for every government. A recent report estimates the cost of data flow restrictions at a GDP loss of around €79bn per year across the European Union or €553bn over 2021-2027.[4]

Initiatives such as that led by the OECD to define high-level principles and safeguards for government access to personal data held by the private sector[5] are urgently needed as an essential first step in addressing cross-border data flow with trust, providing a much-needed foundation that can lead to more scalable measures and global dialogues.

In addition, cooperation between governments and stakeholders including business and multilateral organisations are needed to advocate for interoperable policy frameworks that would facilitate cross-border data flows, enabling data to be exchanged and used in a trusted manner, thereby aiming for high privacy standards.

---

2 Discussion at OECD *CSTP-Korea workshop on Promoting International Technology Co-operation in the Digital Age and in the light of COVID-19* (21-22 September 2020).

3 Hamilton, Daniel D., and Quinlan, Joseph P.: *The Transatlantic Economy 2020* (2020)

4 Frontier Economics: Beyond personal data: The Cost of Data Flow Restrictions to EU Companies

5 Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy

PART 1: Business and cross-border data flows

The ability to transfer data across international borders is critical to companies of all sizes and across all industry sectors.

People who sit on different sides of the globe often need access to the same data, including to coordinate human resources management across global offices, to conduct research and development that spans offices and laboratories, and to trace and recall products regardless of their physical location.

Sending data from one country to another is a core element of both providing and using digital products and now forms the bedrock of international trade in goods and services. At its core, the ability to transfer data across borders ensures that we can access information regardless of our physical location—a critical need that was highlighted by the COVID-19 pandemic, as medical researchers rely on the ability to transfer data across borders to track the spread of the coronavirus and businesses shift to digital tools that let them work remotely and continue serving their customers.

A. Companies in all Sectors Rely on Cross Border Data Flows

Any company with employees, vendors, or offices in more than one country needs to send data internationally every day, including to:

- Manage global inventory through a centralised system, including routing products between countries
- Analyse cybersecurity data in different countries to identify and counter threat and intrusion patterns
- Manage human resources across borders in compliance with relevant legal requirements
- Monitor the performance of products and services distributed globally

Companies in all sectors engage in these ordinary activities, which support businesses of all types. In sectors as diverse as farming, aviation, hospitality, mining, and manufacturing, companies are united in the need to transfer data across international borders. The value of data transfers cuts across industry sectors, with 75% of the value of data transfers accruing to industries like agriculture, logistics, and manufacturing.[6] Indeed, in 2020, the Global Data Alliance, a cross-industry group of companies headquartered around the world formed a coalition to build awareness regarding the importance to international commerce of data transfers and high standards of data responsibility. In real terms, the ability to send data across borders helps companies be more efficient and effective at delivering the products and services their customers' demand.

---

6 McKinsey Global Institute: *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity*, (2011)

ALL INDUSTRIES RELY ON CROSS-BORDER DATA FLOWS

The movement of data across borders is essential to the global economy. Companies in all sectors rely on products and services that require transferring data across international borders.

Agriculture: For farmers, the ability to access cross-border technologies and information can help small-scale producers mitigate crop risks (including losses from pests, disease, and weather-related events) and improve crop yields. It can also ensure those producers have access to up-to-date, reliable information on export markets, pricing, insurance and shipping options, as well as online marketplaces.[7]

Banking & Retail: Detecting credit card fraud at the point of sale is a clear example of the benefit of cross-border data flows. No matter where you are in the world, your bank's computer can analyse your purchases in a matter of seconds after you swipe your credit card. Based on that analysis, the system can allow the purchase or flag it as likely fraud and stop it. Credit card systems also transfer data to detect online or "card-not-present" credit card fraud anywhere in the world.[8]

Health Care & Medicine: Cross-border transfers of personal data allow hospitals and other care facilities to use clinical support software to analyse electronic health records, health insurance claims, and data sets to help caregivers improve effectiveness of medical treatments and reduce risks. For example, analytical software can track and analyse patient outcomes, create medical images and help surgeons and clinicians understand the data and decide when specialists are needed. The software can also be used to share digitised medical images for consultations with specialists anywhere in the world, improving the quality of medical advice for patients.[9]

Transportation & Shipping: When vehicles, vessels, and equipment break down, it can delay production and delivery timelines. Technologies that heavily rely on data flows—such as Internet of Things (IoT), data analytics, AI and blockchain—can help optimise predictive maintenance, avoiding or greatly minimising supply chain disruptions due to transportation delays.[10]

B. Companies of All Sizes Rely on Cross Border Data Flows

Companies large and small rely on the ability to transfer data across borders. Regardless of their size, companies depend on cross-border data flows to deploy tools that support teleworking, virtual collaboration, online training, and the remote delivery of services, such as virtual education and virtual healthcare solutions. These include cloud-based libraries and databases, video conferencing applications, and interactive collaboration platforms that can be leveraged by large and small companies alike.

At the same time, micro, small and medium-sized enterprises (MSMEs) are oftentimes disproportionately affected by regulatory requirements to assess third country data and privacy laws in order to transfer data, as this represents a relatively greater compliance burden on them than on larger companies who have in place dedicated teams to absorb such tasks.

Still, cross-border transfers are critical to many MSMEs, which often rely on global services to reach new markets and serve new customers. As USAID has explained: *"Digital ecosystems have*

---

7 Global Data Alliance: *Cross-Border Data Transfers & Economic Development: Access to Global Markets, Innovation, Finance, Food, and Healthcare*

8 BSA | The Software Alliance: *Cross-Border Data Flows*,

9 BSA | The Software Alliance: *Cross-Border Data Flows*.

10 Global Data Alliance: *Cross-Border Data Transfers & Supply Chain Management*.

the potential to equip informal merchants, women entrepreneurs, smallholder farmers, and MSMEs engaged in cross-border trade with access to markets, information, and finance. These diverse users require trustworthy services that reflect their needs.... [D]igital trade that spans borders depends on free data flows, digitised customs, and innovations in trade finance made possible by new approaches to lending."[11]

Cross-border transfers are also integral to international supply chains, which depend on the ability to move information across borders to optimise sourcing, finance, logistics, risk mitigation, and responsiveness.[12] The supply chain process for most products and services involves many phases, parties and countries—and can involve potentially disruptive external factors like weather, material availability, shortages, geopolitical threats, or emergent health crises.[13] In early 2020, 94 percent of Fortune 1000 companies reported supply chain disruptions from COVID-19,[14] further highlighting the complex and integrated nature of supply chains and the role of data transfers in risk mitigation and response.

CROSS-BORDER ACCESS TO DATA IS CRITICAL FOR SMEs

Cross-border access to marketplaces, purchasers, suppliers, lenders, and other commercial partners enhances the ability of small and medium-sized enterprises to grow and compete.

Leveraging Global Services: Even a single business may need to send data across multiple international borders each day. For example, a small retailer may sell products both through a physical store and through a website that enables it to reach customers in other countries. That retailer may rely on global tools provided by a network of service providers, including cloud storage providers, e-commerce platforms, data analytics providers, human resource management platforms, customer relationship management platforms, and warehousing or fulfilment services that deliver physical goods to customers.[15] Those providers may, in turn, rely on other service providers that distribute services across the globe. Each of these providers can serve a crucial role in ensuring the retailer can reach its customers and deliver products they expect.

Access to Finance: For small businesses, advances in financial transparency and security across developing countries also depend on cross-border access to data and cloud-enabled technologies. Globally, about 1.7 billion adults remain unbanked, with many citing distance from financial institutions as a barrier to obtaining a bank account.[16] Technologies that leverage data transfers can increase access to financial services. These include microlending, in which many local financial institutions use cloud-enabled analytics to determine credit risk profiles and deliver loans through automated processes—resulting in the ability to offer micro-loans to citizens and businesses that would otherwise not have access to credit.[17]

---

11 USAID *Digital Strategy, 2020–2024*,, p. 37.
12 Global Data Alliance: *Cross-Border Data Transfers & Supply Chain Management*
13 According to the AON 2016 Global Climate Catastrophe Report, the supply chain industry faces an average of 260 major natural disasters annually
14 Erik Sherman: *94% of the Fortune 1000 are seeing coronavirus supply chain disruptions: report*, Fortune, 21 February 2020.
15 Future of Privacy Forum: *Understanding Retail Data Flows*, 23 February 2021
16 World Bank: *The Global Findex Database 2017*, Chapter 2: The Unbanked
17 Global Data Alliance: *Cross-Border Data Transfers & Economic Development: Access to Global Markets, Innovation, Finance, Food, and Healthcare*.

C. Economic Benefits

Cross border data flows are important not only because they can help companies access global products and services that protect the security, privacy, and functionality of their information—but also because they have real economic benefits.

Data transfers are estimated to contribute $2.8 trillion to global GDP—a share that exceeds the global trade in goods and is expected to grow to $11 trillion by 2025.[18] With 60% of global GDP digitised by 2022, and growth in every industry driven by data flows and digital technology,[19] disruptions in cross-border data flows have broad consequences that can lead to reduced potential GDP gains, reduced investments in local markets, job losses and negative impacts on local and national digital ecosystems—at a time when every government is striving to prioritise economic recovery.

Governments worldwide appreciate the economic significance of transferring data. In 2021, the G7 emphasised the importance of cross-border transfers, including in the G7 Digital Ministers' Roadmap, which recognises that the "ability to move and protect data across borders is essential for economic growth and innovation."[20] In the United Kingdom, the Minister of State for Media and Data recently described our "hyper-connected world" as "increasingly reliant on data transfers," which underpin everyday conveniences such as GPS navigation, smart home technology, and content streaming services. Yet the value of those transfers extends well beyond convenience. In 2018 the UK exported £190 billion in services delivered digitally and in 2019 investments in the UK tech sector soared to £10.1 billion—a £3.1 billion increase on 2018's figures and the highest level in UK history.[21]

THE ECONOMIC BENEFITS OF CROSS-BORDER DATA FLOWS

Digital tools helped MSMEs across Asia reduce export costs by 82 percent and transaction times by 29 percent, according to a 2019 AlphaBeta Study.[22]

Data localisation measures on Internet of Things (IoT) applications and machine-to-machine data could result in:

- Loss of 59–68 percent of productivity and revenue gains.
- Investment losses ranging from $4–5 billion.
- Job losses ranging from 182,000–372,000 jobs.

Source: 2021 GSMA study conducted in three developing regions (in South America, Southeast Asia and Africa).[23]

According to the World Bank:[24]

- Countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies
- "Restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies and especially on trade in services"

---

18 OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, OECD Digital Economy Papers No. 29724, August 2020
19 Hamilton, Daniel D., and Quinlan, Joseph P.: *The Transatlantic Economy 2020*
20 G7 *Roadmap for Cooperation on Data Free Flow with Trust*, 2021.
21 John Whittingdale MP: *The UK's New, Bold Approach to International Data Transfers*.
22 AlphaBeta, Micro-Revolution: *The New Stakeholders of Trade in APAC*, 2019
23 GSMA: *Cross-border Data Flows — The Impact of Localisation on IOT*, 2021
24 World Bank: *World Development Report*, 2020

According to a 2020 World Economic Forum Study:[25]

- "[A]pproximately half of cross border [services] trade is enabled by digital connectivity [, which] …has allowed developing countries and micro, small and medium sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution."
- "Developing countries…accounted for 29.7% of services exports in 2019."

D. Societal Benefits

When cross-border data flows are restricted, it does not just frustrate companies' efforts to make their products more secure, more privacy protective, and more functional. Restricting data transfers can also prevent governments from delivering timely services to citizens, stifle efforts of medical researchers to collaborating to identify diseases and treatments, and keep individuals from seamlessly communicating with friends, family, and colleagues overseas.

Examples of these societal benefits include:

- **Enabling cross-country collaboration on COVID-19 research**: During the COVID-19 pandemic, trusted collaboration between governments and businesses has enabled researchers to understand the novel coronavirus, identify potential treatments, and develop vaccines more quickly. Such collaborative efforts have been a hallmark of the COVID-10 response, starting with the exchanges of data and genetic viral material, and continuing through the development of databases with genome data, chemical structure data, and clinical studies.[26] This work helps countries respond to the global crisis by increasing understanding of the virus, tracking its spread and the evolution of different variants, and developing and distributing vaccines. Each of these activities requires researchers, governments, and companies to send and receive data across international borders.
- **Improving health care**: Cross-border data transfers can also improve health care generally, particularly for under-served populations. Remote health services and research into new medical treatments depend on cross-border access to data and cloud-enabled technologies, which can enable cross-border consultations between remote providers in one country and specialists and researchers in others, helping those providers improve treatments for non-routine cases. Cross-border access to clinical testing and other biopharmaceutical R&D data can also help researchers study and treat diseases, including not just diseases that are prevalent globally but also rare and neglected diseases.
- **Expanding opportunities for remote work**: The pandemic also illustrated the pivotal nature of data flows in helping companies transition businesses to online-first or online-only models, while shifting employees to remote work. Although many jobs must still be performed on premises, companies are continuing to increase use of remote workplace tools when feasible, while some states are introducing visas for digital nomads to facilitate remote working[27]. Indeed, the exchange of ideas and knowledge among teams of inventors, designers, authors, and other creators and innovators in different countries is critical to all sectors and leveraged by businesses of all sizes.[28]

---

25 WEF: *Paths Towards Free and Trusted Data Flows*, 2020

26 OECD Science, Technology and Innovation outlook 2021: *Times of Crisis and Opportunity, Resolving Global Challenges and Crises Through International Collaboration*

27 Spain's new visa for digital nomads: The key facts

28 OECD Science, Technology and Industry Scoreboard 2017: *The Digital Transformation* (Collaborations may take a variety of forms including international co-inventions involving several firms, both small and large, joint research ventures by private and public entities, and formal and informal networks of scientists).

PART 2: Government access and cross-border data flows: the impact on business

As detailed above, the benefits of trade depend on the trusted and uninterrupted flow of data between countries. Trade, commerce, manufacturing, services, agriculture—virtually any business activity that builds the world's economies—relies on close interaction with commercial partners and customers across the globe and cannot be conducted in national silos alone.

Nevertheless, trust in international data flows is diminishing due to concerns that personal data may be at risk of being accessed by governments across borders, or that governments may lose access to data over which they claim jurisdiction when it is transferred. In 2020 the OECD's Working Party on Data Governance and Privacy (WPDGP) identified unconstrained and disproportionate government access to personal data held by the private sector as a crucial issue for data governance and the protection of individual rights and as a potential barrier to enabling the free flow of data with trust.[29]

WHY DO GOVERNMENTS ACCESS PRIVATE SECTOR DATA?[30]

Driven by rapid digital transformation, governments hold growing amounts of information about individuals. A lot more data (both personal and non-personal) is held by private businesses stored on company servers or by cloud service providers.

Personal data held by the private sector may be valuable for many government purposes, to discover new insights, create knowledge and provide innovative goods and services, such as managing public health matters like the COVID-19 pandemic, optimising public transport grids, or regulating financial markets—just to name a few. Such data is made available through voluntary partnerships.

Among the most important purposes for government access to data are national security and law enforcement. With the advent of cloud computing, much of relevant evidence is commonly held by service providers on private servers located in another country, leading to, what the International Association of Privacy Professionals characterises as the globalisation of criminal evidence.[31] Information such as the content of emails, social network posts, and other content are often stored in a different country. A 2018 report by the European Commission found that *"more than half of all [EU] investigations involve a cross-border request to access [electronic] evidence."*[32] Such data is usually obtained from the private sector through government legal demands.

It is understandable therefore the worldwide exponential increase in recent years in government demands for data held by the private sector. However, this also raises several fundamental questions:

1. In a national context, we must consider to what extent and by what means the state should be entitled to compel access to private organisations' datasets on behalf of the public interest.

---

29 Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy

30 Theodore Christakis, Kenneth Propp, Peter Swire: *Towards OECD Principles for Government Access to Data*

31 IAPP: *The globalization of criminal evidence*, 2018 https://iapp.org/news/a/the-globalization-of-criminal-evidence/

32 European Commission: *Impact Assessment, Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*

2. On an international level, differences in each jurisdiction's approach to laws governing government access, their implementation, and discrepancies in safeguards pose significant complications when data transcends borders. Over the past two decades, and especially since the 2013 Snowden revelations, there has been heightened international scrutiny of intelligence agencies' access to privately held data and the scope and scale of such programs and legal demands. Most recently, the 2015 and 2020 Schrems judgments by the Court of Justice of the European Union (CJEU) terminated data transfers under the EU-U.S. Safe Harbour framework and later the Privacy Shield, asserting that certain U.S. legal authorities for international surveillance did not offer protections equivalent to those required by European law.
3. An added layer of complexity is brought by the lack of common definition of personal data across jurisdictions. The definition of personal data can vary depending on the personal data protection law of each country. Furthermore, it is not always possible to completely separate personal data and non-personal data. Some argue, for example, that most information must be treated as personal data, especially in relation to the GDPR.[33]
4. Third, government access raises tough questions for companies that face these demands for the data they hold. They must decide whether the demand or request is lawful, though the law may be vague, and whether a cross-border demand presents a conflict of law between jurisdictions in which they operate. Government access requests may be for data related to individuals or to businesses located in or business transactions carried out within the governments' jurisdictions. Companies must decide how much information they are compelled to disclose. Furthermore, businesses are faced with the dilemma of what information about their responses to these demands they may disclose to their customers and to the public.[34]

HOW DO GOVERNMENTS ACCESS PRIVATE SECTOR DATA?[35]

Occasionally, governments might **purchase data** from the private sector.

Sometimes, **companies voluntarily provide** national security or law enforcement agencies with data they hold, in case of an imminent threat to the life or safety of an individual or related to another special circumstance. For example, social media platforms might voluntarily identify to a law enforcement agency someone who has shared child pornography or other illegal content online.

Compelled access: In certain cases, law enforcement agencies have the authority to oblige companies to provide access to the data they hold. In democratic countries, law enforcement agencies rely on formal legal process, such as obtaining a judicial warrant or an administrative authorisation. Non-democratic countries, by contrast, might rely on coercion or sanctions or authorities with no independent oversight or accountability.

Direct access: In some situations, intelligence agencies themselves undertake efforts to obtain data held by a private actor without asking the company to provide it and—in nearly all cases—without the private actor even knowing that the government is trying to access the data. This could be carried out, for instance, via signals intelligence and interceptions, covert espionage operations, or hacking.

For the purpose of this paper, we refer to compelled (obliged) access.

---

33 Centre for International Economic Collaboration (CFIEC) Japan: Report of Study Group on Access to Government and Trade Rules, 2022

34 Ira S. Rubinstein, Gregory T. Nojeim, Ronald D. Lee: Systematic Government Access to Private-Sector Data, A Comparative Analysis, Oxford Scholarship Online, 2017

35 Theodore Christakis, Kenneth Propp, Peter Swire: *Towards OECD Principles for Government Access to Data*

There are growing concerns about government practices that fail to preserve trust, namely through unconstrained, unreasonable, or disproportionate requirements that compel access to personal data held by the private sector. Unlimited government access to personal data held by the private sector negatively impacts trust in the digital economy, creating uncertainty with adverse market effects. Fear of such access can cause businesses and organisations to hesitate regarding the transfer to, or storage or processing of personal data in, countries that may allow government access without appropriate safeguards, as this may jeopardise businesses' and organisations' abilities to protect their customers' privacy and to comply with applicable privacy laws.[36] This hesitation does not only affect businesses themselves, but also the populations and economies that cannot benefit (or only at heightened costs) from the products, services, transfer of knowledge and innovation their presence in national markets would bring.

Concerns over government access to personal data significantly contribute to public sectors' reluctance to avail themselves of the benefits of the digital economy, as fears grow that third-party governments will demand access to data over which they previously maintained exclusive control, further eroding trust and burgeoning the negative economic impact. This mistrust could prompt governments to advocate the adoption of rules and practices that require data to be retained locally. Data localisation mandates, however, are harmful for international trade and cooperation:[37]

- Compelled data localisation frustrates the ability of companies to operate in multiple jurisdictions, making it difficult to manage hiring and human resources functions from a single headquarters, to evaluate the performance of connected vehicles from a single research hub, analyse cybersecurity threats at different points in communications networks, and to conduct reasonable network management functionalities, among other challenges (see Part 1 above).
- De facto localisation requirements or compelled data localisation may affect the operations of both multinational companies, and companies that operate in single jurisdictions. Companies that operate in multiple countries may have to consider whether they can provide or continue to provide services in a particular jurisdiction, given the technical implications and costs involved. These concerns are compounded by potential implications for privacy that may arise from putting in place infrastructure that is specific to an individual country. Similarly, companies that operate in a single jurisdiction may be prevented from accessing global products and services and may effectively be cut from global supply chains and, crucially, from foreign markets, stunting their growth and potential. This fragmentation of the internet undermines the economies of scale that is at the core of the digital transformation, including the enablement of micro, small and medium-sized enterprises and the growth of innovation ecosystems domestically.
- Across all industries, the deployment of technical measures broadly and irrespective of the context of a transfer to attempt to limit government access to data can curb the benefits and functionality of a globally interconnected business. Such measures can prevent companies from offering a broad array of features that are critically important to consumers, such as cybersecurity measures or improved communications functionality that depend on the ability to process the underlying data in multiple jurisdictions. These technical measures can also prevent the analysis of data originating from multiple sources in a way that leads to global insights and conclusions, such as combining personal data originated in different countries to implement global safety improvements and increase efficiency.
- Security of data is best achieved with economies of scale arising from investment in robust security protections that apply to cross border data hosting. Per country data localisation solutions cannot achieve those same economies of scale and encourage the use of low-cost solutions that would be sub-optimal given their limited scope.

---

36 Business at OECD: *Statement on Unlimited Government Access to Personal Data Held by the Private Sector: Impact on Cross-Border Data Flows and Economic Growth*, 28 September 2020

37 Business at OECD *Statement on the OECD Committee on Digital Economy Policy's work to develop high-level principles or policy guidance for trusted government access to personal data held by the private sector*, 7 April 2021:

- Data mirroring mandates similarly increase the cost of doing business in a jurisdiction by requiring companies to keep a duplicate copy of data in country. These mandates may assuage local authorities' fears that they will not have timely access to data that is needed in a criminal investigation if it is transferred beyond the state's borders. These measures, however, may also have the underlying goal of ensuring unrestricted and direct access by local authorities, compromising privacy rights and compounding the security risk.
- Ultimately, compelled data localisation is not a solution to resolve the existing conflicts of law that often prevent companies from responding to a foreign government's legitimate law enforcement requests. Instead, compelled data localisation is likely to exacerbate those conflicts and put businesses in an impossible position of arbitrating international legal conflicts, shifting the onus of insufficient regulatory alignment across democratic nations to the private sector.
- There is also a risk that compelled localisation may be used as a tool by governments less committed to the protection of human rights to suppress freedom of expression, privacy, and other fundamental human rights.
- Restrictions on the free flow of data can be accompanied by limitations on the capacity of foreign law enforcement agencies to obtain personal data through lawful requests, which may frustrate governments' law enforcement efforts.
- Requiring data localisation in specific circumstances may reflect a government's perception that it helps meet the law enforcement and national security needs of the country, such as to try to guard public sector data from access by a third-party government. However, as stated above, the movement toward compelled data localisation is ultimately counterproductive toward those and other policy goals and stunts the growth of country's economy and the broader digital economy.

Although the aim of this paper is to discuss compelled access to data held by the private sector, we would also like to take note of the increasing concerns around direct access or source code access, oftentimes linked with nation state or nation state sponsored cyberattacks on private sector infrastructure. For example, a recent report found that government operations resulted in some of the most damaging cyberattacks of late, including indiscriminate and wide-ranging operations conducted by Nobelium and Hafnium.[38] While the economic impact of direct access is less visible (in part because industry employs strong encryption and other security features to prevent direct access and is not involved in this form of access through compulsory processes), there is a clear perception that direct access practices untethered to public standards or accountability can contribute to a lack of trust in cross-border data flows and negatively impact economic output.[39] A recent global survey of more than 500 executives found that nation state attacks are of top concern for executives, with 80% of North-American, 70% of European and 85% of Asia-Pacific executives noting the phenomenon very or somewhat worrisome. The same survey found that respondents see more international economic co-operation as the top geopolitical change that could most reduce nation-state cyber-attacks on private organisations, followed closely by more international political co-operation.[40] Indeed, the private sector is a long-time supporter of establishing and implementing clear international principles and norms for responsible state behaviour in cyberspace. ICC's issue brief on cybersecurity[41] calls for urgent steps that governments must take to curb cyber threats and shield their citizens and economies from the destructive consequences of cyberattacks.

---

38 Microsoft Digital Defense Report, October 2021

39 Business at OECD: Statement on The OECD Process to Develop Common Principles for Trusted Government Access to Data, November 2021

40 Cybersecurity Tech Accord and The Economist Intelligence Unit: Securing a shifting landscape: Corporate perceptions of nation-state threats, February 2021

41 ICC Cybersecurity Issue Brief #1: Call for Government Action on Cybersecurity, 2021

PART 3: Policy recommendations

As discussed in the sections above, the lack of trust in cross-border data flows leads to uncertainty that may discourage the participation of individuals, businesses, and even governments in the global digital economy. Without clear parameters and rules around government access to personal data, including access across international borders, legal uncertainty will persist, likely leading to the proliferation of data localisation measures, which negatively impact the global digital economy. The establishment of rules for government access to private sector held personal data is of immense importance both for business development and social and economic growth.

As the G7 Digital Trade Principles note, *"[a]chieving consensus on common principles for trusted government access to personal data held by the private sector will help to provide transparency and legal certainty. It will support the transfer of data between jurisdictions by commercial entities and result in positive economic and social impacts."* Indeed, trust is strengthened when governments adopt robust and comprehensive commitments to protect the rights and freedoms of individuals, including the fundamental right to privacy, when personal data are subject to government access. Trust is further strengthened when governments work together directly to reduce barriers to cross-border data flows. This includes developing interoperable standards and agreements to address appropriate cross-border legal demands for data and recognising that public sector data should, in general, not be obtained from private sector actors. Principles and safeguards for government access to personal data held by the private sector are therefore urgently needed as an essential first step in addressing cross-border data flow with trust, providing a much-needed foundation that can lead to more scalable measures and global dialogues. In addition, cooperation between governments and stakeholders, including business and multilateral organisations, are needed to advocate for interoperable policy frameworks that would facilitate cross-border data flows, enabling data to be exchanged and used in a trusted manner, thereby aiming for high privacy standards.

The set of seven draft principles currently under discussion in the OECD on compelled government access to personal data held by the private sector offer a promising starting ground towards the establishment of common global rules on obliged access:[42]

1. **Legal bases:** Law enforcement and national security agencies should act under existing legal basis. However, the national legal framework for doing so might be less transparent than applies in the private-sector context. Therefore, the legal framework for obliged access should be publicly available to the greatest extent possible. Furthermore, companies might consider certain demands for data overly sensitive or excessively broad. Although a legal base can be found, the validity of demands needs to be examined carefully.
2. **Pursuit of legitimate aims:** The national legal framework should set out legitimate aims for law enforcement and national security access and ensure that the scope of data acquisition and use is consistent with and proportional to the specified purpose, and documents incidences of access for subsequent oversight and redress purposes.

   This principle ensures that government access has a legitimate purpose, and—if so—the legally protected interests of private individuals are not unnecessarily infringed, and that the infringement of private individuals' rights is limited to what is necessary and reasonable to achieve that purpose.
3. **Requirements for approval:** Governments should have legally established procedural requirements for their access requests that are commensurate with the extent of interference with individual rights. Depending on the seriousness of the interference, prior approval of an access request should be obtained from an independent judicial or administrative body. This would allow for a preliminary review of the fulfilment of the principles relating to compelled government access and help prevent violations of private rights by non-compliant requests.

---

42 Theodore Christakis, Kenneth Propp, Peter Swire: *Towards OECD Principles for Government Access to Data*.

4. **Handling of personal data:** Data obtained through obliged access should be handled in a way that maintains its security and integrity, retained only for so long as legally authorised, and deleted if not authorised for retention. Handling requirements should also be designed to enable oversight bodies to review collection and use.
5. **Transparency:** Government access legal frameworks may be less transparent than is afforded by the private sector. Obliged access regimes should be transparent and publicly available to the greatest extent practicable.

   While individuals have the right to request the disclosure of the data that agencies have collected about them, a government may prevent the disclosure of classified information for a period of time. Nonetheless, the public availability of laws and regulations is an essential element in ensuring that private individuals are aware of the extent to which they will be required to disclose data about themselves and what remedies they may be entitled to. In addition, the disclosure of access information by the state has the significance of providing citizens with oversight to prevent its abuse. Finally, data subject notification ensures that data subjects are informed of their access to data and have the opportunity to seek redress.
6. **Oversight:** Mechanisms should exist for the oversight of obliged access, ensuring reporting and remedying instances of noncompliance. Oversight authorities can conduct impartial investigations and audits and to document their findings through regular reports. Ex-post audits are equally important to prevent violations of the rights of private persons.
7. **Effective redress:** Legally binding remedies should be available to the data subjects in the event of a breach by the government of the access, use and retention rules. Effective redress should be conducted by independent bodies such as courts or other impartial entities. These institutions may require correction or deletion of data, or award compensation for damages. If the information obtained through obliged access is later used in a criminal prosecution, the prosecuted individual should have the right to obtain and challenge it. This notification right may be limited or deferred, "due to legitimate government need to protect the lives and integrity of national persons or national security or law enforcement information and investigations."

In addition to these principles, possible others could be considered, such as:[43]

1. **Conflicts of law:** Government requests for access to data held by a private company in another jurisdiction might pose conflicts of law that are difficult to navigate for businesses. A mechanism should be established through which such conflicts or inconsistencies can be raised and resolved between governments to ensure that compliance with laws and regulations in one jurisdiction does not result in violation of laws and regulations in another. Such mechanism would reduce in advance the burden on private parties to reconcile conflicts between the obligation to provide data under with prohibitions of disclosing data to third parties.
2. **Fairness and equitability:** The operation of the legal system for government access should not be arbitrary but should be carried out with uniform standards and methods. Unfair, arbitrary or discriminatory treatment should be eliminated in the selection of the private sector actors subject to access. Government requests should not be based on prejudice or discrimination on any grounds, such as race, ethnicity, culture, religion, gender or sexual orientation.
3. **Prohibition of excessive costs and burdens:** Government requests should avoid posing excessive costs and burdens on the private company whose data is accessed, thus avoiding impediments to its business operations and infringement of its rights
4. **Intermediary liability:** Governments might request access to companies for user data rather than the users themselves, whereby these companies may be held liable by users for disclosing their personal data, even though companies are obliged to comply with government orders. Similarly, companies may be held liable for the content of user data that they process but do not create themselves. In such cases intermediary liability exemptions should apply.

---

43 Centre for International Economic Collaboration (CFIEC) Japan: Report of Study Group on Access to Government and Trade Rules, 2022

Furthermore, to ensure trust and safety of cross-border data flows, the implementation of commonly agreed global rules and principles on compelled access should be periodically reviewed. This would enable governments to reflect on potential capacity gaps and to improve the business environment accordingly.

Establishing trust and minimising disruptions in data flows are fundamental to reaping the benefits of digitalisation. ICC strongly support the efforts of the OECD to establish common principles for government access to personal data held by the private sector. We stand ready to provide relevant input and evidence to assist with the evaluation of existing practices and timely development of policy guidance that can further trusted government access to data.

ABOUT THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 100 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 **E** icc@iccwbo.org
www.iccwbo.org @iccwbo