Unlocking Public and Private Finance for the Poor

The role of cross-border data flows in the digital economy

In a digital economy, cross-border data flows are crucial in enabling improvements in national economies and living standards in developing countries. Nowadays, the drastic growth in the movement of data means this flow far outweighs the transfer of goods or services. While this means that advances in policy can be made, regulations must be put into place that protect industries, populations, and territories.

The brief, written in close collaboration with Macmillan Keck, seeks to identify specific attributes of cross-border data flows that can help policymakers and regulators build a digital economy that includes — and serves — everyone.

BRIEF

July 2022

Macmillan Keck

Seharish Gillani, Ahmed Dermish, Jeremiah Grossman, and Friederike Rühmann of the UNCDF Policy Accelerator

Summary

Growth in cross-border data flows is outstripping growth in the flow of goods, services, and people. This is enabling improvements in national economies and living standards in developing countries through greater integration into the global economy.

Where data crosses borders, it is exposed to risks beyond such borders, and governments often regulate cross-border data movement to protect their industries, populations, and territories. Data protection laws aim to protect consumer privacy, but inconsistent approaches also impair the ability of consumers to participate fully in the digital economy. Government concerns over national security and public safety have led to restrictions on outward and inward technology and other data transfers. Governments have enacted varying degrees of Internet censorship to block cross-border media and personal communications. Some governments also regulate cross-border data transfers in pursuit of national industrial and fiscal policy.

The global data governance framework is thus currently fractured and inefficient, reflecting deep fissures in trust and instilled differences in approaches among nations. Developing country policymakers cannot alone forge the necessary international cooperation, but they can focus on their domestic data frameworks and participate in relevant international efforts.

Considerations while reading this brief

1. Which challenges related to access to cross-border data flows in a digital economy are most prominent in your market, both a) in general and b) for historically underserved groups such as women and low-income people?

2. Do cross-border data flows policy and regulations in your country address:
   - **Digitization:** The application of cross-border data flows regulation to the digital economy?
   - **Inclusivity:** The specific challenges faced by women, low-income people, and/or other underserved groups with regard to cross-border data flows?

3. Which entities are responsible for regulation cross-border data flows? Are responsibilities clear, and are mechanisms in place to avoid regulatory arbitrage? If not, how could this be improved?

Characteristics and scope

Cross-border data flows encompass any transfer of data or information across sovereign boundaries. Trade in goods and services – and human travel and migration – have involved embedded data flows for millennia. Today, however, cross-border data flows are increasing exponentially.

Cross-border data volumes were 20 times greater in 2017 than in 2007, and they are expected to be four times greater in 2022 than in 2017.[1] The global volume of data stored across the Internet is expected to grow from 33 zettabytes in 2018 to 175 zettabytes in 2025, with nearly half stored in the ***cloud***, a system of globally distributed and connected servers.[2]

Content generated or consumed by humans represents the bulk of cross-border data volume. In 2020, video, gaming, and social sharing comprised 80% of Internet traffic.[3] Data-driven services, such as computing, telecommunications, media, finance, professional services, and others now comprise half of cross-border service trade, roughly equivalent to travel, transport, and other traditional services combined.[4]

Data may flow into, out of, or simply through a country in transit. Border crossings may be intentional (as when a Fiji resident shares files with a Bangladesh resident) or unintentional (as when one Gambian resident emails another Gambian resident but the network routes the message through Europe). A border crossing may occur before a user accesses the data if a global provider has cached copies of content, such as popular social media content, on domestic servers to reduce latency.[5]

Policy drivers and responses

The value of cross-border data flows

Data does not exhibit scarcity characteristics like goods or services.[6] It is sharable, reusable, and non-depletable.[7] Firms can gather, store, process, retrieve, and transmit vast amounts of data at minimal cost. Rather than diminish, data's value grows with repeated access and use due to accretion and network effects: the value of data increases as the volume and variety of data increase and as more users contribute to and have access to it. For example, the aggregation of health and behavioral data relating to individuals allows detection of correlations and possibly causal connections between activities, living conditions, and health. The value of intangibles – or knowledge-based assets[8] – comprises a very large part of total assets in developed economies and can be expected to grow as developing countries' economies rely increasingly on data.[9]

Cross-border flows can improve national economies and living standards in developing countries by leveraging global knowledge to facilitate national integration into the world economy.[10] A 2020 OECD study found that emerging economy participation in the global value chain enabled by cross-border data flows has increased local wages and attracted investment in local infrastructure, machinery, and equipment, even as the share of value added by local intangibles has diminished.[11] Another 2020 OECD study concluded that governments can stimulate local production of intangibles that add value by strengthening their country's appeal for global value chain activities and strengthening local production and innovation ecosystems and connections to

other countries.[12] Achieving these objectives requires openness to cross-border data flows.

The apparel industry offers a good example. A US-based online apparel retailer may procure new patterns from a designer in Italy, review and modify designs in New York, and transmit final patterns to garment manufacturers in El Salvador and Pakistan. The retailer may communicate with carriers for transport of fabrics and other inputs from China, India, and Japan to the garment manufacturers and for transport of completed garments to global distribution centers in Europe and North America. Real-time monitoring of orders and sales can enable the retailer to respond quickly to demand changes by communicating adjustments in style, size, and quantity to the manufacturers.[13]

Cross-border data flows can also help improve public health, agricultural production, and law enforcement. COVID-19 has underscored the importance of global data sharing to monitor the spread and impact of infectious diseases and to develop and administer vaccines and treatments.[14] Technological advances in data collection and analytics can help smallholder farmers in developing countries meet rising food demand in harsher climate conditions.

Data obtained from satellite imagery, on-site measurements of soil conditions, and commodities markets can be combined by computer models to predict supply and demand patterns and crop yields to guide farmers via smartphone applications in selecting seeds, planting, and harvesting.[15] Cross-border data sharing can also help governments address tax avoidance, international crime, and terrorism.[16]

Regulating data flows across borders

As with trade in goods and services and human movement, unregulated cross-border data flows can undermine internal safeguards set up by individual countries to protect their industries, populations, and territories. These threats lead governments to respond by regulating relevant data flows. Sometimes the cross-border nature of data is incidental to underlying concerns, while other times it is the source of those concerns.

Protecting intellectual property to foster innovation and investment

Governments enact ***intellectual property (IP)*** laws to foster investment, innovation, and competition.[17] Developing and bringing valuable knowledge and technology to market often requires significant investment in research and development with uncertain returns. Strong IP laws for copyright, industrial design, patent, trade secrets, trademark, and geographic indication can help developing countries attract inward technology and investment flows.[18]

Copyright, industrial design, and patent laws reward the creation and sharing of information by affording authors, designers, and inventors exclusive economic rights over their published works for limited periods.[19] Responding to data's growing importance, copyright protection was extended to original selections or arrangements of published ***databases*** (collections of data), but not the underlying data, in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).[20] The European Union,[21] Mexico,[22] and South Korea[23] also recognize what are referred to as ***sui generis database*** rights, meaning rights over a

dataset that has been obtained, verified, or presented with substantial investment even if it lacks copyright-worthy originality. Conversely, China,[24] the United States,[25] and other TRIPS parties require originality to protect published databases. A 2020 public consultation by the US Patent and Trademark Office on how IP laws can promote innovation in artificial intelligence received mixed responses about the efficacy of *sui generis* database rights.[26]

Trade secret rights, protecting information that derives commercial value from being kept secret,[27] enable a business to be first-to-market or offer better, faster, or lower-priced goods or services than its rivals. Trade secrets may include raw and processed data derived from collection, observation, measurement, testing, study or survey, formulas, processes, algorithms, productivity tools and methods, and sensitive internal corporate information.[28] Trade secret rights protect firms that invest in research and development, driving digital innovation in market economies. Trademark and geographic indication laws also aim to prevent unfair competition by protecting against counterfeits or inferior imitations.[29] Competition is generally discussed in the Competition Briefing Note.

Within the digital economy, trade secret rights have emerged as a key tool to protect valuable unpublished data.[30] Supply-chain counterparties can, without forfeiting IP protection, share trade secrets in confidence domestically and across borders in the 164 TRIPS contracting states that protect them. A 2014 OECD study of 37 developed and developing countries from 1985 to 2010 found a positive and statistically significant relationship between a country's trade secret protections and economic performance in innovation, international technology transfer, and access to technology-intensive inputs and related products.[31]

Policymakers are reexamining the adequacy of their trade secret protections for the digital economy.[32] Trade secret laws were updated by the European Union[33] and United States[34] in 2016, Japan in 2018,[35] and China in 2019.[36] These trade secret law updates reflect a significant shift of business attention toward data as a key asset in an information economy and recognition by governments that efficient and effective sharing of commercial secrets requires robust legal frameworks to enforce confidentiality undertakings.[37]

The World Intellectual Property Organization (WIPO) unites 193 countries in a global forum for IP services, policy, information, and cooperation to achieve a balanced and effective IP framework.[38] IP rights are recognized at the national level and owners must register their rights (or take other necessary legal steps to ensure their rights will be recognized) in all relevant countries. WIPO administers treaties that harmonize and streamline multinational patent, copyright, and trademark registrations.[39] IP owners rely on national enforcement to protect against license breaches, counterfeiting, and piracy. Restrictions on unlawful cross-border data flows form part of the international IP framework intended to contribute to global innovation and lawful knowledge sharing.[40]

IP owners may license use by others, with or without geographic or other limitations, facilitating global division of supply chain roles. For example, a video copyright owner may restrict where a licensee may view or permit viewing of licensed content. Similarly,

a licensor of machine-readable software code (protected by copyright) may charge licensees based on the number of permitted users and place of use and may elect not to disclose human-readable software code (protected as trade secrets).

IP owners have broad discretion over global distribution and use of their know-how and content. In October 2020, biotech firm Moderna publicly committed not to enforce its mRNA patents against those making vaccines intended to combat COVID-19 and, after the pandemic ends, to license its mRNA patents to others.[41] Responding to this offer, Afrigen Biologics of South Africa has successfully produced its own mRNA vaccine using Moderna technology.[42] In January 2022, Canadian recording artist Neil Young required Sweden-based Spotify, the world's largest music streaming service, to remove his music from its global platform to protest Spotify's decision to carry podcasts by comedian Joe Rogan, who had been accused of promoting COVID-19 vaccine misinformation.[43]

Growth in IP volumes offers one measure of growth in innovation, with trade secrets and patents serving as key measures of digital economy impact. The value or volume of trade secrets cannot easily be measured,[44] but WIPO closely tracks patent applications. 15.9 million patents were in force across 135 jurisdictions in 2020, a 5.9% increase from 2019. In 2020, the five countries with the most patents in force were the United States (3.3 million), China (3.1 million), Japan (2 million), South Korea (1.1 million), and Germany (800,000). In 2020, innovators filed 3.3 million patent applications globally, including 1.5 million in China. Total global applications for unique inventions doubled from 2010 to 2018, reaching 2.1 million. Computer technology was the subject of the most patent applications from 2017 to 2019 in China, the United Kingdom, and the United States, and globally in 2019, with 284,146 published applications. Among large middle-income countries, applicants from India and Mexico filed most heavily in pharmaceuticals, applicants from Brazil in other special machines, and applicants from Turkey in transport. The most African patent applications in 2020 originated in South Africa (915) and Cameroon (672).[45]

Developing countries have long criticized the WIPO framework for enabling foreign firms to appropriate ***indigenous knowledge*** without fairly compensating local populations.[46] The 1993 Biodiversity Convention[47] and 2010 Nagoya Protocol[48] recognize indigenous rights in traditional knowledge and seek reciprocity for sharing. The 1994 Marrakesh Agreement establishing the World Trade Organization (WTO)[49] and the 2001 Doha Declaration[50] address trade-related conflicts. Developing countries now control indigenous knowledge within their borders and are becoming more vigilant in policing its overseas use.[51] In 2009, India put its indigenous medicinal knowledge in the public domain, publishing 200,000 formulas for open use, effectively preventing foreign firms from obtaining patents.[52] Peru recognizes *sui generis* IP rights in indigenous knowledge[53] and actively protects those rights by challenging and invalidating foreign patents.[54] In 2020, Mexico conferred on native communities copyrights in collective works derived from popular culture and traditional indigenous designs, and, in 2021, established fines and imprisonment as penalties for violations.[55] Efforts continue to foster equitable global sharing of indigenous knowledge,[56] which, if preserved and digitized, could help address climate change, disease, and declining biodiversity.[57]

Protecting personal data and privacy

Governments enact data protection laws to provide privacy and consumer protections for their citizens, known as ***data subjects***, whose personal data is collected by ***data controllers*** (which determine the purpose of and means for processing personal data) or processed by ***data processors*** (which process personal data at the direction of or on behalf of a controller). 128 countries have adopted data protection or privacy laws.[58] A compilation of personal data from multiple data subjects comprises a complex array of overlapping and adjacent rights. For example, a data controller may have IP rights with respect to a database, while individual data subjects may have data protection or privacy rights with respect to personal data related to them.

Unlike IP law, data protection currently has no governing global treaty to harmonize national approaches. The 2018 EU General Data Protection Regulation (***GDPR***), replacing the 1995 Data Protection Directive,[59] has in practice become an international model due to the EU's importance in open global markets.[60] The GDPR focuses on providing data subjects (the individuals to whom personal data relates) informed choice over the collection and processing of personal data about them. However, GDPR and many other data protection laws do not afford individuals full ownership or control over personal data about them.[61] These laws impose some obligations on data controllers and processors that override the choice of the data subject[62] while enumerating contexts in which data protection rules may not apply at all.[63]

Many data protection regimes apply to cross-border flows. GDPR applies to (1) foreign processing by EU data controllers; and (2) certain processing by foreign data controllers or processors related to EU data subjects.[64] GDPR prohibits restrictions on lawful data flows within the European Union but not on outward flows.[65] Affirming the benefits of global trade and cooperation,[66] GDPR allows outward data flows consistent with EU protections,[67] expressly permitting transfers to a third country that ensures ***adequate protection***, as determined by the Commission.[68] Personal data may also be transmitted outside the EU if a data controller or processor provides ***appropriate safeguards***.[69] Appropriate safeguards include:

- binding corporate rules (BCR) for transfers within a corporate group or joint venture within which the data may circulate;[70]
- standard contract clauses (SCCs), approved by the Commission or national supervisory authority,[71] to be entered into between the parties sending and receiving the data; or
- certification under an approved mechanism.[72]

At least 14 countries – Argentina, Armenia, Bahrain, Barbados, Brazil, Colombia, Georgia, Israel, Malaysia, Peru, South Africa, Switzerland, Turkey, and Ukraine – have largely followed GDPR in regulating cross-border data flows.[73] Others are more stringent. For example, Algeria[74] and Morocco[75] require prior regulatory approval to ensure the other state provides sufficient legal protection.[76]

Some countries, such as Rwanda, require all personal data to be stored domestically (***data localization***) unless the supervisory authority permits the data controller or processor

to store it outside Rwanda.[77] China allows some outward transfers but requires those processing large amounts to store personal data locally unless they pass a government security assessment.[78] These growing data localization requirements restrict personal data flows across some borders but not others based on origin and destination and contribute to Internet fragmentation.

Absent a multilateral approach, GDPR-based approaches require every country to determine the suitability of cross-border flows to and from every other country. If 194 countries adopted this approach (with 28 EU countries acting as one bloc), over 14,000 bilateral determinations would be required.[79] By January 2022 – a quarter century after the original Data Protection Directive and four years after GDPR[80] – the European Commission had recognized only 14 jurisdictions as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, and Uruguay.[81]

Some regional data protection initiatives have emerged, but none addresses the government-to-government trust issues highlighted by the European Court of Justice (ECJ) in *Schrems* (see box). The 21-member Asia-Pacific Economic Cooperation forum (APEC) developed a Cross-Border Privacy Rules (CBPR) system, with nine participating countries: Australia, Canada, Japan, Mexico, the Philippines, Singapore, South Korea, Taiwan, and the United States.[82] The approach involves self-certification by businesses based on agreed privacy standards, but it does not require public authorities to meet any minimum standard. In January 2021, the Association of Southeast Asian Nations (ASEAN) endorsed a data management framework that includes cross-border data flows as a strategic priority.[83] The African Union Convention on Cyber Security and Personal Data Protection, which has not yet come into force, would set data protection standards but not establish an open internal market among member countries as in Europe, leaving national authorities with sole discretion over cross-border transfers.[84]

In terms of addressing government-to-government trust issues, the OECD Committee on Digital Economy Policy announced in December 2020 plans to convene a drafting group comprising government representatives and experts to examine the possibility of developing an instrument setting out high-level principles or policy guidance for trusted government access to personal data held by the private sector. No outputs from this drafting group have yet been reported.[85] In December 2021, the OECD also published a policy "toolkit" intended to support efforts to achieve greater cross-border interoperability of national privacy and data protection frameworks.[86] Today, international approaches to data protection remain largely fragmented, are not harmonized, and are ineffective.

Developing countries seeking to benefit from the opportunities offered by cross-border flows will need to participate in efforts to simplify and harmonize approaches to such initiatives.

Schrems and the EU-US Safe Harbor

Despite measures to enable cross-border data flows, challenges encountered by the European Union and United States expose inherent barriers absent mutual trust. Under the 1995 Data Protection Directive, the European Commission in July 2000 approved the adequacy of the EU-US Safe Harbor Framework allowing US firms to self-certify compliance with the US Department of Commerce privacy principles.[87]

In 2013, Maximillian Schrems, who lived in Austria, sued the Irish Data Protection Commissioner to bar Facebook Ireland from processing personal data on US servers. On referral from the Irish High Court, the European Court of Justice (ECJ) declared the Commission's adequacy decision invalid in October 2015. The ECJ found that the safe harbor did not bind US public authorities, whose access to personal data was not strictly limited to what was necessary or proportionate for national security. The ECJ held that this violated the privacy and personal data protection rights of EU citizens.[88]

Again acting under the Directive, the European Commission in July 2016 approved the adequacy of the EU-US Privacy Shield, which built on the Safe Harbor privacy principles, with a US Government undertaking to set up an oversight ombudsperson independent of the intelligence community.[89]

On another referral from the Irish High Court in the ongoing Schrems litigation, the ECJ in July 2020 applied GDPR provisions to invalidate the Commission's adequacy decision. The ECJ found that Privacy Shield did not adequately protect EU citizens' privacy from data processing by US public authorities and the ombudsperson scheme did not guarantee an effective remedy or fair trial.[90] The ECJ also cast doubt on whether standard contract clauses could provide appropriate safeguards.[91]

Ensuring national security and public safety

Government concerns over national security and public safety have led to extensive restrictions on outward technology transfers. For over 70 years, governments have restricted weapons technology transfers to hostile actors.[92] Some 28 non-proliferation treaties are now in force.[93] Four multilateral non-proliferation frameworks also subsist. Strict adherence means limiting outward transfers of ***dual-use technology***, i.e., technology that can be used for both peaceful and military applications. Export controls on technology can harm potential recipient countries in the near term and the restricting country's economic competitiveness in the long term.[95]

Governments are also concerned about international cybersecurity – preventing hostile foreign actors from intercepting or compromising valuable data or using international communications channels to perpetrate terrorism and crime. Cybersecurity is discussed generally in the Cybersecurity Briefing Note. In 2020, financial gain was the primary cyberattack motive, and criminal organizations were behind 80% of attacks.[96] Typical government responses are to strengthen local criminal laws and law enforcement capability,

improve international cooperation, establish Computer Emergency Response Teams (CERTs), and educate businesses and citizens.[97] Among international efforts is the Financial Action Task Force to combat money laundering and terrorist finance by helping national authorities trace fund flows. Its 37 member countries include rapidly developing economies such as Argentina, China, India, Indonesia (observer), Mexico, Russia, South Africa, and Turkey.[98]

Although state actors perpetrate fewer than 10% of documented cyberattacks,[99] governments are concerned about cybersecurity threats from state actors and state-sponsored or state-harbored private actors.[100] Canada's government considers nation-states the most sophisticated threat actors, with dedicated resources and personnel, extensive planning and coordination, and working relationships with private actors and criminals.[101] US experts say the line between nation-state and criminal actors is blurring, as nation-states harbour and rely on criminal proxies to project power.[102] There is growing concern over the theft of trade secrets by foreign actors who access data in the cloud and in networks.[103] Some state actors[104] engage in cybercrime to support weapons programs and other UN-sanctioned activities.[105]

As part of their response, some governments now restrict routing and ownership of networks used for cross-border data transmission considered vulnerable to state-sponsored surveillance, interception, and disruption.[106] National security concerns have also been cited to block equipment and installation suppliers.[107]

Concern about foreign state actors is also the primary justification offered by the European Union, China, and a growing list of countries for data localization requirements that restrict outward flows of personal data. In *Schrems* (see box), the ECJ focused on the risk of US national security agencies processing EU citizen data. China's 2021 Data Security Law prohibits the transfer of Chinese personal data to foreign judicial or enforcement authorities without government approval.[108] The logical extension of such measures is to restrict domestic data processing by foreign-owned firms, especially as some countries extend the reach of their intelligence and law enforcement agencies to personal data held in other countries. For example, difficulties encountered by the US Government in 2013 using a search warrant to obtain access to data held by Microsoft in a data center in Ireland led to changes in US law in 2018 requiring US data providers to disclose overseas data within their control.[109] France's cybersecurity chief has since advocated for Europe to exclude US cloud providers – Google, Amazon, Facebook, Apple, and Microsoft – from handling sensitive personal data.[110] Even where such measures are in place, however, state-sponsored espionage can employ spyware to clandestinely reach across borders and capture data.[111]

The Russian invasion of Ukraine in February 2022 led to the stiffest international sanctions and restrictions on cross-border data flows ever imposed.[112] These included EU exclusion of key Russian banks from the cross-border payment messaging system operated by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)[113] and voluntary cut-offs of Russia by private international payment networks such as American Express, Mastercard, and Visa.[114] Still, by mid-March 2022, the European Union, United States, and other

allies had not prohibited information services from making themselves accessible within Russia. Influenced in part by a desire to keep Russian citizens informed in the face of state media misinformation, information service providers such as Akamai (content caching), Amazon Web Services (cloud computing), Cloudflare (data centers), Facebook (social media), Telegram (messaging), Twitter (social media), and WhatsApp (messaging) continued to operate in Russia.[115]

Regulating objectionable content

By its nature, the Internet permits access to vast volumes of online content from other countries. Some governments use technology extensively to filter what content may enter and leave the country. During the first month of the February 2022 invasion of Ukraine, Russia blocked over 270 foreign news and financial sites.[116]

The Universal Declaration of Human Rights enshrines the right to freedom of opinion and expression without interference and the right to seek, receive, and impart information and ideas through any media and regardless of frontiers.[117] This right is subject to limitations to secure due recognition and respect for rights and freedoms of others and to establish just requirements of morality, public order, and the general welfare in a democratic society.[118]

Different governments have enacted varying degrees of Internet censorship in interpreting and implementing these limitations. At one end of the spectrum, the United States and others impose few restrictions on online speech.[119] At the other end, China, Eritrea, North Korea, Saudi Arabia, Turkmenistan, and others strictly limit speech.[120] In the middle are countries like Papua New Guinea, which prohibits the publication of ***objectionable content***, which it defines to include content that promotes or incites terrorism or offensively portrays sex, drug use, crime, cruelty, blasphemy, immorality, violence, or revolting or abhorrent phenomena.[121]

Pursuing national industrial and fiscal policy

Some governments are exploring ways to regulate cross-border data activities in pursuit of national industrial and fiscal policy.

India, among other developing countries, has adopted a data localization policy that is currently reflected in a series of sector-specific laws and regulations and may soon be more broadly included in pending data protection legislation, first proposed in 2019 and likely to become law in 2022.[122] One rationale offered for the requirement is to generate economic growth and employment opportunities by increasing the likelihood that value-adding data processing occurs within India rather than the country merely supplying raw data to global platforms. A 2021 quantitative assessment of the bill's likely impact under various scenarios found that a localization framework involving local data storage and global processing would best enable the envisioned economic growth, but the overall GDP impact was unclear if local data storage equipment needed to be imported.[123] A 2014 economic simulation suggested that the impact on India's GDP might in fact be negative.[124]

In the same vein, the European Union has begun to express its desire for ***digital sovereignty*** – to become less dependent on US and Chinese technology firms.[125] The notion has various objectives, according to the European Council. A central objective is to build a digital single market. Another is to reinforce Europe's ability to define its

own rules, make autonomous technological choices, and develop and deploy strategic digital capacities and infrastructure, while safeguarding its values, fundamental rights, security, and social balance. The EU also seeks to leverage its tools and regulatory powers to help shape global rules and standards, remaining open only to firms complying with EU rules and standards.[126]

Data localization also has fiscal implications, making it easier for national revenue authorities operating under traditional tax regimes based on physical presence to tax data processing services provided by foreign firms.[127] However, the international digital services tax framework, approved by 136 countries in October 2021, may help to close the tax gap without the disadvantages of data localization by re-allocating some taxing rights over larger multinational enterprises from their home countries to markets where they have digital business activities and earn profits.[128]

Developing an international data governance framework

The current global ***data governance*** framework[129] is fractured and inefficient (with the exception of the WIPO intellectual property framework), reflecting deep fissures in trust and inherent differences in approach among both allied and non-allied nations.

Cross-border data flows have traditionally been addressed in trade agreements. WIPO and the WTO thus offer established fora for improving data governance in the trade context. But this has so far been insufficient. WIPO's mission is limited to intellectual property, while WTO has lost influence due to increasing trade protectionism, criticism that the TRIPS patent provisions limit access to medicines in developing countries, and the reemergence of competing bilateral and multilateral trade blocs.[130]

In its 2021 World Development Report, the World Bank called on governments to forge new domestic social contracts for data and cooperate internationally in harmonizing and coordinating data governance.[131] At the World Economic Forum 2019 annual meeting, Japan's Prime Minister invited leaders to build an international order for Data Free Flow with Trust (DFFT). Leaders at the 2020 annual meeting provided multistakeholder input on global data governance processes needed to realize the benefits of increased cross border data flows. The World Economic Forum has recently published a white paper with the following five key groups of recommendations:

1. Governments should establish personal data protection and trusted mechanisms for cross-border transfer;
2. Governments should refrain from restricting non-personal information and machine-to-machine data, and they should cooperate on the development and implementation of legislation on governmental access to digital information abroad for law enforcement;
3. Stakeholders should engage in market-led technical standardization;
4. Governments should pursue international trade negotiations on various matters relating to data; and
5. Developed economy governments, businesses, and international organizations should provide technical assistance to developing countries to develop high standards for data protection, ensuring the costs do not impede micro, small, and medium enterprises from participating in global trade.[132]

Meanwhile, developing country policymakers cannot forge the necessary international cooperation alone, but they can focus on their domestic data frameworks, as suggested by the World Bank. They can also participate in relevant international efforts. For instance, eTrade for All seeks to inform developing countries of the opportunities for digital trade and access to technical assistance.[133] Countries can set their sights on economic opportunities relating to cross-border data by embracing international standards, as Mauritius has done by enacting robust data protection legislation and signing the Council of Europe's Convention 108+ for the Protection of Individuals with Regard to the Processing of Personal Data.[134] In Asia, the APEC CBPR system provides a framework for participating countries to enable cross-border data flows, including in the context of digital trade.[135] The African Continental Free Trade Agreement negotiations underway under the auspices of the African Union also include a component on digital trade.[136]

Emerging topics

Web3 (or Web 3.0) is a concept for a new iteration of the World Wide Web based on blockchain technology. It would decentralize the Internet and afford users greater ability to participate in the governance and operation of the protocols governing their user experience, both as sources and recipients of data. Some believe Web3 could improve data security, scalability, and privacy beyond what is currently possible with Web 2.0 platforms. Some have identified risks with the self-governance, such as vulnerability to hacking of smart contracts, cryptojacking, lack of regulatory best practices, questions about the quality and policing of information, manipulation of data in Web3 apps, and risks to mobile wallets including loss of funds.[137] At present, Web3 is currently limited to niche applications for cryptocurrencies.[138]

Additional resources

Resources for further reading

- UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economic Report 2021
- How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, ITIF
- We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty, Internet & Jurisdiction Policy Network
- Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, World Economic Forum
- A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, World Economic Forum
- Cross-Border Data Flows: Realising benefits and removing barriers, GSMA

Organizations

- United Nations Conference on Trade and Development (UNCTAD)
- World Trade Organization (WTO)
- World Intellectual Property Organization (WIPO)
- Organisation for Economic Co-operation and Development (OECD)
- G-20
- World Economic Forum (WEF)
- Global Data Alliance
- International Society of Chief Data Officers

Notes

[1] World Bank, World Development Report 2021: Data for Better Lives at 237 (2021). Available at https://openknowledge.worldbank.org/handle/10986/35218.

[2] David Reinsel, John Gantz & John Rydning, Data age 2025: The Digitization of the World, from Edge to Core, IDC White Paper at 3-4 (IDC, Nov 2018). Available at https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

[3] Sandvine, The Global Internet Phenomena Report at 4 (May 2020). Available at https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%2020200507.pdf.

[4] World Bank, World Development Report 2021: Data for Better Lives, supra, at 238.

[5] For a discussion of the concepts of where data is and how it moves, see, e.g., Javier Lopez Gonzalez, "Hitchhiker's Guide to Cross-Border Data Flows," Opinion (OECD, 3 Jun 2019). Available at https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/.

[6] See James Heskett, "What Happens When the Economics of Scarcity Meets the Economics of Abundance?" Working Knowledge (Harvard Business School, 4 Aug 2006). Available at https://hbswk.hbs.edu/item/what-happens-when-the-economics-of-scarcity-meets-the-economics-of-abundance.

[7] See United Nations Conference on Trade and Development (UNCTAD), Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, Box 1.1 at 6 (2021). Available at https://unctad.org/system/files/official-document/der2021_en.pdf.

[8] See, e.g., Ali Alsamawi, Charles Cadestin, Alexander Jaax, Joaquim José Martins Guilhoto, Sébastien Miroudot & Carmen Zürcher, Returns to intangible capital in global value chains: New evidence on trends and policy determinants §2.1 at 7, DSTI/CIIE(2020)27/FINAL (OECD, 5 Nov 2020). Available at https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CIIE(2020)27/FINAL&docLanguage=En.

[9] The value of intangibles held by major US-listed companies grew from USD 122 billion in 1975 to USD 21 trillion in 2018, rising from 17% of total assets in 1975 to 90% in 2020. Intangible asset value in 2020 reached 75% of total asset value in Europe, 57% in Korea, 44% in China and 32% in Japan. Ocean Tomo, Intellectual Asset Market Value Study (Ocean Tomo LLC, 2022) (assessing firms included in the S&P 500 in the United States, S&P Europe 350, KOSDAQ in Korea, Shanghai Shenzhen CSI 300 and Japan's Nikkei-225). Available at https://www.oceantomo.com/intangible-asset-market-value-study/.

[10] See, e.g., Joshua Meltzer & Peter Lovelock, Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia, Global Economy & Development Working Paper 113 (Brookings, Mar 2018). Available at https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf.

[11] Ali Alsamawi et al., Returns to intangible capital in global value chains: New evidence on trends and policy determinants, supra, §4.2 at 24-26.

[12] Ari Van Assche, Trade, investment and intangibles: The ABCs of global value chain-oriented policies, TAD/TC/WP(2020)5/FINAL (OECD, 23 Nov 2020). Available at https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)5/FINAL&docLanguage=En.

[13] The example in the main text is hypothetical and overly simplifies the supply-chain elements and role of data flows. For a more thorough and generic analysis of cross-border data flows in sourcing, manufacturing and distribution, see Swedish National Board of Trade, No Transfer, No Production – a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods (Mar 2015). Available at https://unctad.org/system/files/non-official-document/dtl_ict4d2016c02_Kommerskollegium_en.pdf.

[14] For a discussion of the benefits and barriers to cross-border sharing of public health data, see Marco Liverani, Srey Teng, Minh Sat Le & Richard Coker, "Sharing public health data and information across borders: lessons from Southeast Asia." Global Health at 14 (Springer Nature, 29 Sep 2018). Available at https://globalizationandhealth.biomedcentral.com/articles/10.1186/s12992-018-0415-0.

[15] For a discussion of the potential of digital technologies to help small-hold farmers, see Kenneth Iversen, Hoi Wai, Jackie Cheng, Kristinn Helgason & Marcelo LaFleur, "Frontier technologies for smallholder farmers: addressing information asymmetries and deficiencies," Frontier Technology Issues (UN Department of Economic and Social Affairs, 17 Nov 2021). Available at https://www.un.org/development/desa/dpad/publication/frontier-technology-issues-frontier-technologies-for-smallholder-farmers-addressing-information-asymmetries-and-deficiencies/.

[16] For example, the UN Convention against Transnational and Organized Crime and the protocols thereto, with 143 signatories and 190 parties, contains multiple articles for improving international cooperation in law enforcement through data sharing. See United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, opened for signature 12 Dec 2000 (entered into force on 29 Sep 2003). Available at https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

[17] See, e.g., WTO > Trade Topics > TRIPS > What are IPRs (2022). Available at https://www.wto.org/english/tratop_e/trips_e/intel1_e.htm.

[18] See, e.g., Keith Maskus, "Intellectual Property: Balancing Incentives with Competitive Access," in Global Economic Prospects and the Developing Countries at 129 (World Bank, 2002). Available at https://openknowledge.worldbank.org/handle/10986/14050.

[19] See WTO Secretariat, Primer 1: Economic Concept Relevant to Intellectual Property Rights at 2-3, The Economics of Trips Series (WTO, undated). Available at https://www.wto.org/english/tratop_e/trips_e/trips_econprimer1_e.pdf.

[20] See Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), opened for signature 15 Apr 1994, art. 10.2 (entered into force 1 Jan 1995 and amended on 23 Jan 2017), appended as Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, opened for signature in Marrakesh, Morocco on 15 Apr 1994 (entered into force 1 Jan 1995). Available at https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm. Article 10.2 requires that databases under copyright where the selection or arrangement of their contents constitute intellectual creations.

[21] See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases art. 7 (1996). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009.

[22] See Mexico Federal Copyright Law art. 108 (Ley Federal del Derecho de Autor) (originally published in the Official Gazette of the Federation on 24 Dec 1996, as amended through 1 Jul 2020) (affording creators of non-original databases protection for 5 years from the date of publication). Available at https://wipolex.wipo.int/en/text/579009.

[23] See South Korea Copyright Act arts. 91-98 (originally enacted by Act No. 8101 on 28 Dec 2006, as amended through 21 Mar 2017) (affording creators of non-original databases protection for 5 years from the next year after publication) Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42726&lang=ENG.

[24] See Copyright Law of the People's Republic of China art. 14 (originally adopted at the 15th Meeting of the Standing Committee of the Seventh National People's Congress on 7 Sep, 1990 and promulgated by Order No. 31 of the President of the People's Republic of China on 7 Sep 1990, as amended). Available at http://www.asianlii.org/cn/legis/cen/laws/cloproc372/.

[25] See US Copyright Act of 1976, 17 U.S.C. §§101("compilation"), 103(b) et seq. (enacted by Pub. L. No. 94-553, 90 Stat. 2541, 19 Oct 1976, as amended). Available at https://www.law.cornell.edu/uscode/text/17/chapter-1.

[26] See US Patent and Trademark Office, Public Views on Artificial Intelligence and Intellectual Property Policy (Oct 2020). Available at https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf.

[27] Article 39.2 of the TRIPS Agreement requires undisclosed information to benefit from protection if the information (1) is secret, (2) has commercial value because it is secret and (3) has been subject to reasonable steps to keep it secret. The TRIPS Agreement does not require undisclosed information to be treated as a form of property, but does require that a person lawfully in control of such information have the possibility of preventing it from being disclosed to, acquired by or used by others without his or her consent in a manner contrary to honest commercial practices, such as breach or inducement to breach contract or confidence, or acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in its acquisition.

[28] See, e.g., Pricewaterhouse Coopers, The scale and impact of industrial espionage and theft of trade secrets through cyber at 10 (European Commission, Dec 2018). Available at https://ec.europa.eu/docsroom/documents/34841/attachments/1/translations/en/renditions/native.

[29] See, e.g., WTO > Trade Topics > TRIPS > What are IPRs, supra.

[30] See, e.g., Interview by WIPO Magazine with Francis Gurry, Director General, WIPO (Oct 2019). Available at https://www.wipo.int/wipo_magazine/en/2019/05/article_0001.html.

[31] Douglas Lippoldt & Mark Schultz, "Uncovering Trade Secrets - An Empirical Assessment of Economic Implications of Protection for Undisclosed Data," OECD Trade Policy Papers, No. 167 (OECD Publishing, 2014). Available here.

[32] See Interview by WIPO Magazine with Francis Gurry, Director General, WIPO, supra (Oct 2019).

[33] See Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

[34] See US Defend Trade Secrets Act of 2016, 18 U.S.C. §1386 (added by Pub. L. No. 114-153, 11 May 2016, 130 Stat. 376). Available at https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf.

[35] See Japan Unfair Competition Prevention Act, Act No. 47 of 1993, as amended by Amendment of Act No. 33 of 2018 and prior amending Acts (2018). Unofficial English translation available at http://www.japaneselawtranslation.go.jp/law/detail/?id=3629&vm=02&re=02.

[36] See Anti-Unfair Competition Law of the People's Republic of China art. 9 (Adopted at the 3rd Meeting of the Standing Committee of the Eighth National People's Congress on 2 September 1993, revised at the 30th Meeting of the Standing Committee of the Twelfth National People's Congress on 4 November 2017, and amended in accordance with the Decision on Revising the Construction Law of the People's Republic of China and Other Seven Laws at the 10th Meeting of the Standing Committee of the Thirteenth National People's Congress on 23 April 2019). Unofficial English translation available at https://wipolex.wipo.int/en/text/547027.

[37] See, e.g., International Chamber of Commerce, Protecting Trade Secrets – Recent EU and US Reforms at 5-6 (ICC, 2019). Available at https://iccwbo.org/content/uploads/sites/3/2019/04/final-icc-report-protecting-trade-secrets.pdf.

[38] WIPO > About WIPO (2022). Available at https://www.wipo.int/about-wipo/en/.

[39] See, generally, WIPO > About IP > Copyright, available at https://www.wipo.int/copyright/en/; WIPO > About IP > Patents, available at https://www.wipo.int/patents/en/; WIPO > About IP > Trademarks, available at https://www.wipo.int/trademarks/en/.

[40] For a discussion of the elements of the complex elements comprising the international legal framework for IP, see Henning Grosse Ruse-Khan, "Intellectual Property and International Law: A Research Framework," in Irene Calboli and Maria Lillà Montagnani, eds., Handbook of Intellectual Property Research: Lenses, Methods, and Perspectives (Oxford University Press, Sep 2021). Available at https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198826743.001.0001/oso-9780198826743-chapter-2.

[41] See Statement by Moderna on Intellectual Property Matters during the COVID-19 Pandemic (Moderna, 8 Oct 2020) (listing 10 patents for mRNA-1273 COVID-19 vaccine issued in the United States and registered in foreign jurisdictions). Available at https://investors.modernatx.com/Statements--Perspectives/Statements--Perspectives-Details/2020/Statement-by-Moderna-on-Intellectual-Property-Matters-during-the-COVID-19-Pandemic/default.aspx.

[42] See "Covid: South Africa makes its own version of Moderna vaccine," BBC News (BBC, 4 Feb 2022). Available at https://www.bbc.com/news/health-60258088.

[43] See Ben Sisario, "Spotify Is Removing Neil Young Songs After He Complains of 'Misinformation,'" The New York Times (26 Jan 2022). Available at https://www.nytimes.com/2022/01/26/arts/music/spotify-neil-young-joe-rogan.html.

[44] See David S. Almeling, "Seven Reasons Why Trade Secrets Are Increasingly Important," 27 BERKELEY TECHNOLOGY LAW JOURNAL 1091, 1093 (University of California, 2012). Available at https://lawcat.berkeley.edu/record/1125065/files/fulltext.pdf.

[45] See WIPO, World Intellectual Property Indicators 2021 at 11-22 (World Intellectual Property Organization, 2021). Available at https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2021.pdf.

[46] See, e.g., Ian Vincent McGonigle, "Patenting nature or protecting culture? Ethnopharmacology and indigenous intellectual property rights," 3 JOURNAL OF LAW AND THE BIOSCIENCES 217 (Oxford University Press, 2016). Available at https://academic.oup.com/jlb/article/3/1/217/1751287.

[47] The Convention on Biological Diversity, opened for signature 5 Jun 1992, art. 18 (entered into force 29 Dec 1993). Available at https://www.cbd.int/convention/articles/?a=cbd-18.

[48] Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity, opened for signature 29 Oct 2010 (entered into force 12 Oct 2014). Available at https://www.cbd.int/abs/text/.

[49] See TRIPS Agreement art. 27.3(b).

[50] Doha Declaration on the TRIPS Agreement and Public Health, adopted by the WTO Ministerial Conference of 2001 in Doha on 14 Nov 2001. Available at https://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_trips_e.htm.

[51] For one perspective on the tensions between free information flows and preserving and protecting traditional knowledge, see Professor Dr. Erica-Irene A. Daes, "The impact of globalization on Indigenous Intellectual Property and Cultures," Lecture at Museum of Sydney, Sydney, Australia (25 May 2004). Available at https://humanrights.gov.au/about/news/speeches/impact-globalization-indigenous-intellectual-property-and-cultures.

[52] See Randeep Ramesh, "India moves to protect traditional medicines from foreign patents," The Guardian (22 Feb 2009). Available at https://www.theguardian.com/world/2009/feb/22/india-protect-traditional-medicines. India published an extensive database of the traditional remedies to serve as a check against bio-prospectors.

[53] WIPO, Intellectual Property and Traditional Knowledge, WIPO Publication No. 920, Booklet No. 2 at 21-22 (2005). Available at https://www.wipo.int/edocs/pubdocs/en/tk/920/wipo_pub_920.pdf.

[54] See Nicolás Gutiérrez, "Latin America - How Latin America countries protect their traditional knowledge through IP," News Article (European Commission, 16 Jan 2020) (discussing Peru's successful challenges to patent validity in Europe and Japan). Available at https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/how-latin-america-countries-protect-their-traditional-knowledge-through-ip-2020-01-16_en.

[55] See Amy Guthrie, "Mexico Fights Cultural Appropriation with New Intellectual Property Law," Law.Com (ALM Media Properties, 6 Dec 2021). Available at https://www.law.com/international-edition/2021/12/06/mexico-fights-cultural-appropriation-with-new-intellectual-property-law/.

[56] See WIPO > WIPO Media Center > Background Briefs > Traditional Knowledge and Intellectual Property (2022). Available at https://www.wipo.int/pressroom/en/briefs/tk_ip.html.

[57] See, e.g., J. Michael Finger & Philip Schuler, eds., Poor People's Knowledge: Promoting Intellectual Property in Developing Countries (World Bank & Oxford University Press, 2004). Available at https://openknowledge.worldbank.org/bitstream/handle/10986/15049/284100PAPER0Poor0peoples0knowledge.pdf?sequence=1. See also Indigenous Knowledge: Local Pathways to Global Development (World Bank, 2004). Available at https://documents1.worldbank.org/curated/en/981551468340249344/pdf/307350ENGLISH0ik0local0pathways.pdf.

[58] UNCTAD > Data Protection and Privacy Legislation Worldwide (2021). Available at https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[59] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL#d1e1384-1-1. As noted in its title, the GDPR repealed and replaced the EU's 1995 Data Protection Directive. Directive 95/46/EC. Though consistent with the 1995 objectives and principles, the GDPR sought, among other goals, to address fragmentation in interpretation and enforcement that had arisen within the European Union. See GDPR recital 9.

[60] See Elizabeth M. Renieris, "The GDPR at Two — Global Floor or Global Ceiling?" Berkman Klein Center Collection (Medium, 9 Jul 2020). Available at https://medium.com/berkman-klein-center/the-gdpr-at-two-global-floor-or-global-ceiling-9dc9a43d1780.

[61] For a discussion of the relationship between personal data rights and IP rights, see, for example, Leon Trakman, Robert Walters & Bruno Zeller, "Is Privacy and Personal Data Set to Become the New Intellectual Property?" INTERNATIONAL REVIEW OF INTELLECTUAL PROPERTY AND COMPETITION LAW, University of New South Wales Research Paper No. 19-70 (3 Sep 2019). Available at https://ssrn.com/abstract=3448959.

[62] For example, recital 39 of the GDPR lays out multiple data protection requirements that are non-negotiable, meaning that data controllers and processors are automatically bound by those requirements regardless of whatever consent-based arrangements they make with data subjects. These non-negotiable requirements include requirements that (1) any processing of personal data must be lawful and fair, (2) specific transparency and disclosure standards must be satisfied, (3) the scope personal data processed must be limited to the purposes for which it is processed, (4) limit the period for which personal data is stored and require disclosure of the time limit to data subjects, (5) permit the processing of personal data only if the purpose of the processing could not be fulfilled by other means, (6) require every reasonable step be taken to rectify or delete inaccurate personal data, and (7) ensure appropriate confidentiality and security during processing of personal data. Similarly, Recital 86 mandates that a data controller notify data subjects of data breaches.

[63] For example, the GDPR disapplies its data protection provisions to (1) activities regarding national and common security (recital 16), (2) data processing by natural persons in the context of personal or household activities (recital 18), (3) criminal prosecution (recital 19), (4) anonymous data (recital 26), (5) data of deceased persons (recital 27), (6) public authorities in connection with their official tasks (recital 31) and certain other contexts.

[64] GDPR recitals 23 & 24 & art. 3. The GDPR also applies in circumstances where EU member state law applies under international law, such as activities within overseas embassies and consular offices, but these circumstances are typically very limited in scope and impact and therefore not considered in the current discussion.

[65] GDPR art. 1.3.

[66] GDPR recital 101.

[67] GDPR art. 44.

[68] GDPR art. 45. The determination is made by the Commission in accordance with criteria set out in article 45.

[69] GDPR art. 46. Appropriate safeguards are only required for transfer of data to a third country which has not been found to provide adequate protection under article 45.

[70] The requirement for binding corporate rules are set out in GDPR art. 47.

[71] GDPR art. 46.2(a), (c), (d) or (e).

[72] GDPR arts. 42.2 & 46.2(f).

[73] See UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 124 & note 10.

[74] Algeria Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data art. 44. Available in French at https://www.joradp.dz/FTP/JO-FRANCAIS/2018/F2018034.pdf.

[75] Morocco Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data art. 43. Available in French at https://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf.

[76] See UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 124 & note 11.

[77] Rwanda Law relating to the protection of personal data and privacy, Nº 058/2021 of 13/10/2021, art. 50 (published in the Official Gazette on 15 Oct 2021). Available at https://www.minijust.gov.rw/fileadmin/user_upload/Minijust/Publications/Official_Gazette/_2021_Official_Gazettes/October/OG_Special_of_15.10.2021_Amakuru_bwite.pdf.

[78] Personal Information Protection Law of the People's Republic of China art. 40 (Passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021) (effective 1 Nov 2021). English translation available at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[79] The number of bilateral determinations with 167 countries involved would equal the sum of 166+165+164+ . . . +3+2+1 = 167(167+1)/2 = 14,028.

[80] See UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 104-105.

[81] See European Commission > Law > Law by topic > Data protection > International dimension of data protection > Adequacy decisions. (2022). Available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[82] Cross Border Privacy Rules System > Government (2022). Available at http://cbprs.org/government/.

[83] ASEAN Data Management Framework: Data governance and protection throughout the data lifecycle, Final Copy Endorsed by the 1st ASEAN Digital Senior Officials' Meeting (Jan 2021). Available at https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf.

[84] The African Union Convention on Cyber Security and Personal Data Protection, opened for signature 27 Jun 2014, art. 12.2(k) (not yet entered into force). Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. In addition, the African Convention will not come into force until signed and ratified by at least 15 states. See Yarik Turianskyi, Africa and Europe: Cyber Governance Lessons, Policy Insights 77 at 2 (South African Institute of International Affairs, Jan 2020). Available at https://media.africaportal.org/documents/Policy-Insights-77-turianskyi.pdf. But as of the date of last signature only 14 of 55 African Union member states had signed and only eight had ratified it. See African Union, List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection (last updated 18 Jun 2020). Available at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

[85] OECD, Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy (Dec 2020). Available at https://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm.

[86] See Lisa Robinson, Kosuke Kizawa & Elettra Ronchi, "Interoperability of privacy and data protection frameworks," Going Digital Toolkit Note, No. 21 (OECD, 8 Dec 2021). Available at http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf.

[87] 2000/520/EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. Available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520.

[88] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, EU:C:2015:650 (2015) (citing Articles 7 (privacy right) and 8 (personal data protection right) of the European Charter of Fundamental Rights). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362.

[89] 2016/1215/EU, Commission Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

[90] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, EU:C:2020:559 (2020) (citing Article 47 of the European Charter of Fundamental Rights). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&from=en.

[91] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, supra, ¶¶122-149.

[92] In 1949, NATO set up the Coordinating Committee for Multilateral Export Controls (COCOM), establishing an export licensing regime administered by participating countries to prevent the Soviet Union from acquiring critical dual-use technology for its military. See William Alan Reinsch & Emily Benson, Digitizing Export Controls: A Trade Compliance Technology Stack? (Center for Strategic and International Studies, Dec 2021). Available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211201_Reinsch_Digitizing_ExportControls.pdf?EZ.7BrxaXtjvnwfiD79RZ5ptWs692Ua6.

[93] For a listing of disarmament treaties and their status, see United Nations Office of Disarmament Affairs > Disarmament Treaties Database (2022). Available at https://treaties.unoda.org/.

[94] These four international groups include the following: (1) The 48-member Nuclear Suppliers Group established in 1974. See Nuclear Supplier Group > About (2022). Available at https://www.nuclearsuppliersgroup.org/en/about-nsg. The NSG includes all members of the "nuclear club," major economies and some developing countries such as Argentina, Belarus, Brazil, Bulgaria, China, Croatia, Cyprus, Kazakhstan, Mexico, South Africa and Turkey among others. (2) The 42-member Australia Group established in 1985 and focused on biological and chemical weapons. See The Australia Group > Home (2022). Available at https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html. (3) The 35-member Missile Technology Control Regime established in 1987. See MTCR > Home (2022). Available at https://mtcr.info/. (4) The 42-member Wassenaar Arrangement established in 1996 and focused on conventional arms and dual-use technologies. The framework is formally known as The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies See The Wassenaar Arrangement > About Us (2022). Available at https://www.wassenaar.org/about-us/. The Wassenaar Arrangement is the successor of COCOM.

[95] See, e.g., Stephen Ezell & Caleb Foote, How Stringent Export Controls on Emerging Technologies Would Harm the U.S. Economy (Information Technology & Innovation Foundation, May 2019). Available at https://www2.itif.org/2019-export-controls.pdf.

[96] See Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto & Suzanne Widup, 2021 Data Breach Investigations Report at 12 (Verizon, 2021). Available at https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.

[97] See, e.g., Pricewaterhouse Coopers, The scale and impact of industrial espionage and theft of trade secrets through cyber, supra, at 12.

[98] See FATF > About (2022). Available at https://www.fatf-gafi.org/about/.

[99] See Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto & Suzanne Widup, 2021 Data Breach Investigations Report at 12

[100] A 2020 intelligence report found Germany was a recurring target of state-sponsored political espionage, industrial espionage and terrorism, singling out Russia, China, Iran and Turkey as primary aggressors. See German Federal Ministry of the Interior (Bundesamt für Verfassungsschutz), Building and Community, 2020 Report on the Protection of the Constitution: Facts and Trends at 39-45 (15 Jun 2021). Available at https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2021-06-brief-summary-2020-report-on-the-protection-of-the-constitution.pdf?__blob=publicationFile&v=11.

[101] See Canadian Centre for Cyber Security > Publications > Cyber threat and cyber threat actors (last updated 29 Jun 2021). Available at https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

[102] Testimony of Mieke Eoyang, US Deputy Assistant Secretary of Defense for Cyber Policy, hearings of Armed Services Committee, US House of Representatives (14 May 2021), reported by C. Todd Lopez, "In Cyber, Differentiating Between State Actors, Criminals Is a Blur," DOD News (US Department of Defense, 14 May 2021). Available at https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/.

[103] See, e.g., US Government, Administration Strategy on Mitigating the Theft of US Trade Secrets at 3-5 & 7-10 (Feb 2013). Available at https://www.justice.gov/criminal-ccips/file/938321/download, and Interview by Pete Williams, NBC News, with Christopher Wray, Director, US Federal Bureau of Investigation, Washington, DC (1 Feb 2022). Available at https://www.nbcnews.com/politics/politics-news/fbi-director-wray-says-scale-chinese-spying-us-blew-away-rcna14369.

[104] See United Nations Panel of Experts on the Democratic People's Republic of Korea established pursuant to UN Security Council resolution 1874 of 2009, Report on Democratic People's Republic of Korea, S2021/211 at ¶¶156-166 (4 Mar 2021). Available at https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf.

[105] See Gabriel Bassett, et al., 2021 Data Breach Investigations Report, supra, at 13.

[106] Substantial tensions have arisen in relation to international networks used for data transmission in relation to concerns over unlawful monitoring or interception of data by other governments. See, e.g., Douglas Main, "Undersea Cables Transport 99 Percent of International Data," Newsweek (2 Apr 2015). Available at https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072. See also, US Department of Justice, Office of Public Affairs, "Team Telecom Recommends FCC Grant Google and Meta Licenses for Undersea Cable," Press Release (17 Dec 2021). Available at https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable. See also US Federal Communications Commission, Non-Streamlined Submarine Cable Landing License Applications Accepted for Filing, Report No. SCL-00328NS, Public Notice (13 Aug 2021). Available at https://docs.fcc.gov/public/attachments/DOC-374897A1.pdf.

[107] In 2020, efforts to block technology supplied by Chinese firms such as Huawei and ZTE were extended to 5G technology via the US-led Clean Network initiative which now includes over 30 major mobile operators from 20 countries. See, e.g., Roslyn Layton, "State Department's 5G Clean Network Club Gains Members Quickly," Forbes (4 Sep 2020). Available at https://www.forbes.com/sites/roslynlayton/2020/09/04/state-departments-5g-clean-network-club-gains-members-quickly/?sh=48ee7e387536. Similar issues have arisen in relation to financing of submarine cables. See, e.g., Ethan Meick, Michelle Ker & Han May Chan, China's Engagement in the Pacific Islands: Implications for the United States, US-China Economic and Security Review Commission, Staff Research Report at 10 (14 Jun 2018). Available at https://www.uscc.gov/sites/default/files/Research/China-Pacific%20Islands%20Staff%20Report.pdf. David Wroe, "Australia refuses to connect to undersea cable built by

Chinese company," The Sydney Morning Herald (26 Jul 2017). Available at https://www.smh.com.au/politics/federal/australia-refuses-to-connect-to-undersea-cable-built-by-chinese-company-20170726-gxj9bf.html.

[108] Data Security Law of the People's Republic of China, as adopted at the 29th session of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on June 10, 2021 (entered into force on 1 Sep 2021) (official Chinese text and unofficial English translation). Available at https://www.cov.com/-/media/files/corporate/publications/file_repository/data-security-law-bilingual.pdf. See also Luo, Yan. "China Enacts Data Security Law." Inside Privacy (14 Jul 2021). Available at www.insideprivacy.com/cybersecurity-2/china-enacts-data-security-law.

[109] US-based Microsoft maintains a data center in Ireland for customers in Europe. In 2013, the US government served a search warrant on Microsoft for data associated with a European subscriber's msn.com email account. The warrant was issued under the US Stored Communications Act, 18 U.S.C. Chap. 119 §§ 2701 et seq. These Stored Communications Act provisions were originally adopted as part of the Omnibus Crime Control and Safe Streets Act of 1968, added by Pub. L. No. 90–351, title III, § 802, 19 Jun 1968, 82 Stat. 212. The current text and legislative history are available at https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119. After a US appeals court held in 2016 that Microsoft need not comply if the data was stored outside the United States, US law was amended in 2018 to require US service providers to disclose overseas data in their control. Microsoft Corp v. United States (In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp), 829 F.3d 197 (2d Cir. 2016). Available at https://casetext.com/case/microsoft-corp-v-united-states-in-re-a-warrant-to-search-a-certain-endashmail-account-controlled-maintained-by-microsoft-corp. See also, Clarifying Lawful Overseas Use of Data Act §103(a)(1), 18 U.S.C. §2713 (added by Pub. L. 115–141, div. V, § 103(a)(1), 23 Mar 2018, 132 Stat. 1214). Available at https://www.justice.gov/dag/page/file/1152896/download.

[110] See Laurens Cerulus, "France wants cyber rule to curb US access to EU data," Politico (13 Sep 2021). Available at https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.

[111] Pegasus spyware, developed by Israeli firm NSO Group, has reportedly been used unlawfully to surveil public officials and citizens in Armenia, Azerbaijan, Bahrain, Finland, Germany, Hungary, India, Israel, Jordan, Kazakhstan, Mexico, Morocco, Panama, Palestine, Poland, Rwanda, Saudi Arabia, Spain, Togo, Uganda, United Arab Emirates, United States and Yemen. See Stephen Shankland, "Pegasus spyware on State Department phones: What you need to know," cnet (3 Dec 2021). Available at https://www.cnet.com/tech/mobile/pegasus-spyware-on-state-department-phones-what-you-need-to-know/. Pegasus can be covertly installed on mobile phones and other devices and capture data stored on those devices, such as texts, voice messages, passwords, location and app data and turn on the microphone or camera.

[112] See, e.g., "Factbox: Putin's Russia hit with wall of international sanctions after Ukraine invasion," Reuters (7 Mar 2022). Available at https://www.reuters.com/markets/europe/putins-russia-hit-with-wall-international-sanctions-after-ukraine-invasion-2022-03-07/.

[113] See, e.g., Philip Blenkinsop, "EU bars 7 Russian banks from SWIFT, but spares those in energy," Reuters (2 Mar 2022). Available at https://www.reuters.com/business/finance/eu-excludes-seven-russian-banks-swift-official-journal-2022-03-02/.

[114] See, e.g., "Visa and Mastercard suspend Russian operations," BBC News (6 Mar 2022). Available at https://www.bbc.com/news/business-60637429.

[115] See, e.g., Frank Bajak & Barbara Ortutay, "War censorship exposes Putin's leaky internet controls," AP News (13 Mar 2022). Available at https://apnews.com/article/russia-ukraine-putin-technology-business-europe-1b8fec033200c33a2aef83b3d2d18713.

[116] Frank Bajak & Barbara Ortutay, "War censorship exposes Putin's leaky internet controls," supra.

[117] This rights is set out in Article 19 of the Universal Declaration of Human Rights proclaimed by UN General Assembly resolution in 1948. See United Nations > About Us > Universal Declaration of Human Rights art. 19 (2022). Available at https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[118] Universal Declaration of Human Rights art. 29.

[119] Section 230 of the US Communications Decency Act largely protects online platforms from liability for user content. See 47 U.S.C. §230(c)(2). Available at https://www.govinfo.gov/content/pkg/USCODE-2020-title47/pdf/USCODE-2020-title47-chap5-subchapII-partI-sec230.pdf. See also Frances Burwell, "Free speech and online content: What can the US learn from Europe?" New Atlanticist (Atlantic Council, 1 Feb 2021). Available at https://www.atlanticcouncil.org/blogs/new-atlanticist/free-speech-and-online-content-what-can-the-us-learn-from-europe/.

[120] On China, see Beina Xu & Eleanor Albert, "Media Censorship in China," Backgrounder (Council of Foreign Relations, last updated 17 Feb 2017). Available at https://www.cfr.org/backgrounder/media-censorship-china. On Eritrea, see Committee to Protect Journalists, "10 Most Censored Countries," Special Report (10 Sep 2019). Available at https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/#1. On North Korea, see Freedom House, Freedom in the World 2022: North Korea (accessed 18 Mar 2022). Available at https://freedomhouse.org/country/north-korea/freedom-world/2022. On Saudi Arabia, see Freedom House, Freedom in the World 2021: Saudi Arabia (accessed 18 Mar 2022). Available at https://freedomhouse.org/country/saudi-arabia/freedom-world/2021. On Turkmenistan, see International Partnership for Human Rights, "Turkmenistan: new internet restrictions, new cases of persecution of outspoken activists" (4 May 2021). Available at https://www.iphronline.org/turkmenistan-dec_20_mar_21.html.

[121] See Papua New Guinea Classification of Publications (Censorship) Act No. 18 of 1989 as amended. Available at http://www.paclii.org/pg/legis/consol_act/copa1989393/.

[122] See, e.g., Stephen Pritchard, "India's Personal Data Privacy Bill: What does it mean for individuals and businesses?" The Daily Swig (23 Feb 2022). Available at https://portswigger.net/daily-swig/indias-personal-data-privacy-bill-what-does-it-mean-for-individuals-and-businesses.

[123] See Anirudh Burman & Upasana Sharma, How Would Data Localization Benefit India? Carnegie India Working Paper at 30 (Carnegie Endowment for International Peace, Apr 2021). Available at https://carnegieendowment.org/files/202104-Burman_Sharma_DataLocalization_final.pdf.

[124] See Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel & Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery," ECIPE Occasional Paper No. 3/2014 (European Centre for International Political Economy, 2014). Available at https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1047.8696&rep=rep1&type=pdf.

[125] See UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 105.

[126] See General Secretariat of the Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, Note to Delegations, EUCO 13/20 ¶7 at 4 (2 Oct 2020). Available at https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.

[127] See, e.g., "Data localisation – protection or protectionism?" The Hindu BusinessLine (8 Aug 2021). Available at https://www.thehindubusinessline.com/business-laws/data-localisation-protection-or-protectionism/article35801546.ece.

[128] See OECD/G20 Base Erosion and Profit Shifting Project, Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy (8 Oct 2021). Available at https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf.

[129] This document uses the term data governance in the same sense as the World Bank, namely to describe the policy, legal and regulatory framework governing data collection, transmission, storage, processing, use and deletion, both within and across borders. The term has also long been used in another sense by data professionals to describe the exercise of authority and control (planning, monitoring and enforcement) in managing an enterprise's data assets.See Susan Earley, ed., The DAMA Dictionary of Data Management (DAMA International, 2nd ed., 2011). Available at https://www.dama.org/cpages/body-of-knowledge (purchase required). DAMA International is a not-for-profit, vendor-independent, global association of technical and business professionals dedicated to advancing the concepts and practices of information and data management.

[130] James McBride & Anshu Siripurapu, "What's Next for the WTO?" Backgrounder (Council on Foreign Relations, updated 13 Dec 2021). Available at https://www.cfr.org/backgrounder/whats-next-wto.

[131] World Bank, World Development Report 2021: Data for Better Lives, supra, at xi-xii.

[132] World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, White Paper at 17 (World Economic Forum, May 2020). Available at https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.

[133] See https://etradeforall.org/.

[134] "Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data." Council of Europe, Strasbourg. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[135] See end notes 82 and 83 above.

[136] See https://au.int/en/cfta.

[137] See, e.g., Pablo Blanco, "Web3 Security and its Cybersecurity Risks," 22 April 2022. Available at https://www.rootstrap.com/blog/web3-security-and-the-cybersecurity-risks/.

[138] See, e.g., Ethereum > Developers > Docs > Foundational Topics > WEB2 VS WEB3 (last edited 11 Dec 2021). Available at https://ethereum.org/en/developers/docs/web2-vs-web3/.

About UNCDF

The UN Capital Development Fund makes public and private finance work for the poor in the world's 46 least developed countries (LDCs). UNCDF offers "last mile" finance models that unlock public and private resources, especially at the domestic level, to reduce poverty and support local economic development. UNCDF pursues innovative financing solutions through: (1) financial inclusion, which expands the opportunities for individuals, households, and small and medium-sized enterprises to participate in the local economy, while also providing differentiated products for women and men so they can climb out of poverty and manage their financial lives; (2) local development finance, which shows how fiscal decentralization, innovative municipal finance, and structured project finance can drive public and private funding that underpins local economic expansion, women's economic empowerment, climate adaptation, and sustainable development; and (3) a least developed countries investment platform that deploys a tailored set of financial instruments to a growing pipeline of impactful projects in the "missing middle."

The UNCDF Policy Accelerator works with governments to help them create policies and regulations that include everyone in the digital economy, shares practical tools and guides based on our technical assistance model and our go-to resources, and provides scholarships to policymakers and regulators to study with our world-class partner organisations.

About Macmillan Keck

Macmillan Keck Attorneys & Solicitors advises clients on strategy, advocacy, deals, controversies and reforms in the digital economy. The firm's clients include telecom operators, digital financial service providers, online health and education providers, other digital content, application and service providers, governments and sector and competition regulatory authorities, and international organisations. The firm has successfully completed numerous complex projects across a majority of countries in every continent.

Disclaimer

This publication was last reviewed in July 2022.

Unlocking Public and Private Finance for the Poor

policy.accelerator@uncdf.org

policyaccelerator.uncdf.org | uncdf.org

FIND US