PECC Signature Project on the Digital Economy

Primer on Economic Integration Issues Posed by the Digital Economy

22 October 2021

Contents

This Primer is the product of a signature project of the Pacific Economic Cooperation Council led by the New Zealand Committee of the Pacific Economic Cooperation Council (NZPECC) We express our great appreciation to the members of the Advisory Group for their inputs to the report. The views expressed in the report are the author's alone and are not necessarily the views of PECC, or its member committees. PECC neither endorses the views in this publication, nor vouches for the accuracy or completeness of the information contained within the publication. PECC accepts no liability for any loss, damage, or expense arising out of, or in connection with, any reliance on any omissions or inaccuracies in the material contained in this publication.

Acronyms

ACCC	Australian Consumer Competition Commission
AI	Artificial Intelligence
AIDC	AI Data Consortium
ALP	Arm's Length Principle
AML/CFT	Anti-Money Laundering and Counter-Terrorism Financing
AMS	ASEAN Member States
APEC	Asia Pacific Economic Cooperation
API	Application Programming Interface
APTs	Advanced Persistent Threats
ASEAN	Association of Southeast Asian Nations
AWGIPC	ASEAN Working Group on Intellectual Property Cooperation
BPS	Badan Pusat Statistik, or Statistics Indonesia
CAD	Computer-Aided Design
CBPR	Cross-Border Privacy Rules
CDN	Content Delivery Network
CDP	Central Depository of the Singapore Exchange
CDR	Consumer Data Right
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CMA	Competition and Markets Authority, UK
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSA	Cyber Security Agency, Singapore
CSP	Cloud Service Provider
DCP	Data Collaboratives Program
DEPA	Digital Economy Partnership Agreement
DMA	Digital Markets Act of the European Commission
DMF	Data Management Framework
DSA	Digital Services Act of the European Commission
EDI	Electronic Data Interchange
EMVCo	Europay, Mastercard, and Visa (Consortium)
eID	Electronic Identification
ESG	Environmental, Social and Governance
EU	European Union
FAANG	Facebook, Apple, Amazon, Netflix, Google
FEAT	Fairness, Ethics, Accountability and Transparency
FIDO	Fast IDentity Online
FTA	Free Trade Agreements
FTC	Federal Trade Commission
G20	Group of 20
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GHGs	Green House Gasses
GNU-GPL	GNU General Public License
GVC	Global Value Chain
IATA	International Air Transport Association
ICT	Information and Communications Technology
IDC	International Data Corporation
IEC	International Electrotechnical Commission
IIAs	International Investment Agreements

IMDA	Infocomm Media Development Authority, Singapore
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
IPRs	Intellectual Property Rights
IPRED	Directive on the Enforcement of IP Rights
ISO	International Organization for Standardization
ISPs	Internet Service Providers
IT	Information Technology
ITU	International Telecommunications Union
JTC	Joint Technical Committee
KFTC	Korea Fair Trade Commission
MAS	Monetary Authority of Singapore
MCC	Model Contractual Clauses
MPD	Mobile Positioning Data
MSME	Micro, Small and Medium Enterprise
NATFA	North American Free Trade Agreement
NDI	National Digital Identity
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NPSP	National Public Service Portal
ODA	Overseas Development Assistance
OECD	Organization for Economic Co-operation and Development
OTT	Over-the-Top
PDPA	Personal Data Protection Act
PDPC	Personal Data Protection Commission
PECC	Pacific Economic Cooperation Council
POFMA	Protection from Online Falsehoods and Manipulation Act
OASIS	Online Aerospace Supplier Information System
QoS	Quality of Service
QR	Quick Response
RCEP	Regional Comprehensive Economic Partnership
SADEA	Singapore-Australia Digital Economy Agreement
SGX	Singapore Exchange
SIPS	Singapore IP Strategy
SME	Small Medium Enterprise
SRI	Socially Responsible Investing
STAN	Singapore Tourism Analytics Network
STB	Singapore Tourism Board
SVCs	Supply Value Chains
SVOD	Subscription Video-on-Demand
TC	Technical Committee
TRIPS	Trade-Related Aspects of Intellectual Property Rights
TPGs	Transfer Pricing Guidelines
UGCP	User-Generated Content Providers
UK	United Kingdom
UN	United Nations
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UNCTAD	United Nations Conference on Trade and Development
UN/EDIFACT	United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport
US	United States

USMCA	United States-Mexico-Canada Agreement
VOD	Video-on-Demand
WCO	World Customs Organization
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
ZB	Zettabyte

Glossary

5G	5G is shorthand for the fifth generation of mobile telecommunications technology, with greater bandwidth, giving higher download speeds. Increasingly, there is greater scope for delivering existing and new services along narrower spectrum frequencies, at faster speeds.
Additive manufacturing	Additive manufacturing, or 3D printing, is the reproduction of a digitally created object in a physical medium, such as plastic, metal or even living tissue.
Advanced Persistent Threats	Advanced Persistent Threats (APTs) are cyber-attacks facilitated by jurisdictions with the aim of conducting espionage, data theft or infrastructure destruction, often using coordinated groups of threat actors.
Aggregators	Aggregators provide services that aggregate data (compiling, sorting, and re-packaging datasets) to intermediate the relationship between users and third parties. Aggregators often provide commercial platform services within the scope of their business and often have a critical mass of users and leverage access to those users to extract value from third parties.[1] Aggregators include search engines such as Google or Bing, video platforms such as YouTube, and social networks such as Facebook.
Artificial Intelligence	Artificial intelligence (AI) is the general catch-all term for computing systems that emulate human cognitive functions, such as identifying patterns to solve problems, and comprises machine learning, deep learning, big-data analytics, augmented intelligence, automation, and some types of robotics.
Augmented intelligence	Augmented intelligence is the supplementing of human decision-making with further information derived from artificial intelligence. In work contexts, it empowers humans to work in a more efficient and informed manner.
Automation	Automation is the use of machines to replace or reduce human involvement in repetitive tasks. In tandem with developments in AI, this increasingly refers to the "application of technology to monitor and control the production and delivery of products and services."[2] Urban mass transit systems are an example of automation.
Big data	Big data is digital data from multiple sources. Big data analytics involves advanced analytic techniques being deployed to interpret massive, diverse datasets from different sources, of varying size, and varying data types.
Blockchain technology	Blockchain, or distributed ledger technology, is a shared ledger that facilitates the recording of transactions or digital assets in a network (or, 'immutable' chain), rendering the history of the asset transparent. Since it is decentralized, the asset can be accessed or traded in real time. Almost anything can be tracked on a blockchain network. Blockchain is fundamental to cryptocurrency.
Caching service	Caching is the process of storing copies of files in temporary storage location so that they can be accessed more quickly. Caching services speed up access to information that has been retrieved previously, because the cache server is physically closer to the user.
Cloud computing	A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., server hosting, data, applications and services storage) that can be rapidly made available with minimal management requirement, usually on a subscription fee basis. Cloud computing has enabled

[1] Ben Thompson (2019) A Framework for Regulating Competition on the Internet, https://stratechery.com/2019/a-framework-for-regulating-competition-on-the-internet

[2] International Society of Automation (2009) What is Automation?, www.isa.org/about-isa/what-is-automation

	organizations of all sizes and types, and governments to be able to outsource their information technology systems and requirements to specialist third party providers.
Cloud service provider (CSP)	A provider of cloud services to a cloud service customer.
Conduit service	Consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.
Content moderation	Content moderation refers to the practice by online platforms to screen user-generated content and ensure that the published content does not violate rules and guidelines against prohibited, illegal or inappropriate content, such as content related to copyright infringement, child pornography, violence or instigating violence against certain groups, hate speech, harassment, calls for terrorism, and misinformation. Content moderation includes takedown demands, such as formal requests from governments to remove content.
Cross-border data flows	Cross-border data flows are movements of data across borders and are key to any form of digital trade. It is integral to e-commerce and enables the use of emergent data-driven technologies such as additive manufacturing, cloud computing and AI, all of which have potential transformative effects on economic development and trade.
Cryptocurrency	A cryptocurrency is a digital currency that is secured by cryptography on a decentralized network based on blockchain technology. Cryptocurrencies are not issued by any central bank or authority, meaning that in theory, they are not subject to government monetary policy.
Cybersecurity	Cybersecurity is the protection of organizations, individuals and networks from digital attacks. Digital attacks may involve the unauthorized access, modification and extraction of data, the theft of proprietary information, and the purposeful incapacitation of critical infrastructure.
Data center	Data centers are dedicated spaces that host computer systems and related components, including communications devices and storage systems. They are key aspects of digital infrastructure, though they need not always be physically present locally for government and business operations to run smoothly and securely.
Data controllers	Individuals or organizations which have decision-making authority over the purpose and means by which data is processed.[3] Data controllers may independently collect data from data subjects, or they may purchase or otherwise acquire data from other data controllers. Regardless of the source of their data, data controllers bear the greatest responsibility and liability for the storage and security of data assets—as well as the greatest degree of agency with regards to accessing, processing, or transforming it. In some frameworks data controllers are referred to as 'data owners'. Scenarios exist where more than one entity can exert decision making authority over data, such as in the context of cloud computing, where both cloud service providers and users are able to exert certain degrees of control over data. In such cases all associated entities are joint controllers, with ownership clarified through legal instruments between them. Data controllers could include government agencies with access to citizens' data, or businesses who have been granted data access by their

[3] European Commission (2021) What is a data controller or a data processor?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

	customers, such as Facebook.
Data localization	Data localization is the storing of data in the jurisdiction from which it originates. The term has come to be associated with regulations or legal requirements for data to be resident in the economy of origination or control. In some contexts this is seen as warranted, such as if the compromise of certain sensitive data would threaten the internal stability of an economy, cause demonstrable long-term damage to the economy, result in immediate and exceptionally grave damage to the effectiveness of defense and security, intelligence operations, or crime prevention. However, it is not always the case that privacy and/or security is enhanced by stipulating where data is located. See also data sovereignty.
Data processors	Individuals or organizations which are instructed to process personal data on behalf of controllers. Whether as entities external to the data controller, or as components of the data controlling entity itself, data processors function to process, modify and transform data in accordance with instructions from controllers. Data processors do not own the data they process, unless they are also controllers, but have access to the data for the purposes of processing it. Examples of data processors include cloud service providers such as Alibaba Cloud, Amazon Web Services, and Google Cloud Platform.
Data sharing	Data sharing refers to the ability to access, use and reuse data in a safe and commercially viable manner. This includes open government initiatives as well as data sharing among businesses. Such initiatives are seen as a levelling mechanism, with potential to even out market imbalances which would otherwise endow private entities that control significant proprietary data resources with disproportionate market power.
Data sovereignty	Data sovereignty refers to the notion that economies within which data is collected, held, or processed are able to use their laws and regulatory structures to access, hold legal jurisdiction, or otherwise affect the data in question. The concept is premised on the belief of being able to enact sovereign rights (i.e., control or ownership) over data assets which are understood to be intrinsic or inalienably attributable to their originating jurisdictions.
Data subjects	Individuals to whom data can be attributed, directly or indirectly. Data subjects are the basis for data, which can relate to their physical, physiological, genetic, mental, economic, cultural, or social identity.[4] The terminological basis for data subjects originated with the GDPR, with other jurisdictions often using less specific terminology, such as 'individuals' or 'users', within their data protection or data access frameworks.
Data transfer mechanisms	Data transfer mechanisms are legal mechanisms that bridge differences in data protection and privacy regimes without necessarily requiring domestic laws or regulations to be revised. They include certifications and data transfer agreements between economies and/or organizations. These mechanisms seek to facilitate interoperability across data protection/privacy regimes, easing compliance costs for businesses whilst ensuring the safe and secure flow of data. The ASEAN Data Management Framework (DMF) and Model Contractual Clauses (MCCs) for Cross-Border Data Flows constitute data transfer mechanisms.
Deep learning	Deep learning is a branch of artificial intelligence and machine learning. Deep learning algorithms can take in and process unlabeled, unstructured data such

[4] GDPR-info.eu (2021) Definitions, https://gdpr-info.eu/art-4-gdpr

	as text and images to 'learn' in an unsupervised manner. Self-driving cars, for example, use deep learning to optimize their functionality.[5]
Digital divide	The digital divide is the disparity between those with excellent connectivity to digital infrastructure, and those who remain outside the reach of this infrastructure, with the ensuring difference in access to goods, and services from both private and public sectors.
Digital economy	The digital economy encompasses all sectors of the economy that rely upon or use Internet Protocol (IP)-enabled networks and platforms as part of the embedded infrastructure of the society. In fully digitalized economies this includes all major sectors of the economy and society.
Digital identities	A digital identity is "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions".[6] A digital identity can uniquely identify a person, and can be distinguished from an online identity, which is not unique. A digital identity can refer to a person, a legal entity such as an enterprise, or to a thing (such as a financial asset).
Digital regulatory arbitrage	Digital regulatory arbitrage occurs when different jurisdictions create different sets of digital laws and regulations, and persons or corporate entities that operate across borders can take advantage of whichever offers the greater benefits.
Digital signatures	A digital signature is an algorithm used to validate the authenticity and integrity of a message such as a transaction, or a document. This signature is unique to a person or entity and ensures that the digital message has not been altered since it was signed.
Digital single window	Digital single windows are portals or other online methods to consolidate disparate trade processes within a single standardized process, form or entity, and which can be submitted electronically. These lower the barriers to trade considerably and promote growth across economies. These can be implemented at the economy level, or more ambitiously and effectively, at a regional level, as in the example of the ASEAN Single Window.
Digital trade	Digital trade encompasses the increasing digitalization undergirding most facets of trade: the use of digital technologies in supply chains and logistics, the invention of new, commercially valuable communications and market access channels, and the value of the data that is created, transferred, and processed. It includes digital goods and services, digital delivery (full or partial) of tangible goods and services, digital enablers of trade, and emerging digital technologies.
Digital trade standards	Standards are typically published documents outlining specifications, procedures or regulations to ensure consistent implementation of processes, technologies, and methods. They can enable a high benchmark for security, safety, quality and reliability of goods and services being delivered into a market. The standards-setting process can be faster and more organic than the development of regulations, and can often respond with agility to changing technological, business, and regulatory conditions due to the range of participants and levels of expertise involved in the international standards-setting process.
Digital transformation	Digital transformation is the point at which the accretion of digitalization processes—the moving of physical processes in business, trade, and

[5] NVIDIA (2021) Deep Learning, https://developer.nvidia.com/deep-learning

[6] GSMA, World Bank Group, and Secure Identity Alliance (2016) Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

	government—reaches a point of constituting a 'new normal' or paradigm shift. This can occur within an institution such as a business or government agency, as well as within an economy or society more widely.
E-commerce	E-commerce, or 'electronic commerce,' is the buying and selling of goods, services and/or data on the Internet, potentially including digital delivery of goods or services. Such transactions can be B2C (business to consumer, such as by Amazon or Alibaba), B2B (business to business), C2C (consumer to consumer, such as by eBay or Carousell), and B2G (business to government).
E-invoicing	E-invoicing is the process of electronically delivering invoices in a standardized format. E-invoices can be automatically imported into the buying organization's accounts payable system, representing a large acceleration of business practices from paper-based systems.
Green digitalization	Green digitalization encompasses new ways to create environmentally sustainable 'green' growth. Examples include ways to monitor and reduce energy consumption in smart homes, the replacement of oil and gas driven vehicles with electric or hydrogen-fueled vehicles controlled by digital operating systems, and the carbon-reducing industrial processes that replace electrical-mechanical with digitally controlled production processes.
Hosting service	Consists of the storage of information provided by, and at the request of, a recipient of the service. Online platforms are a sub-category of hosting services.
Industry 4.0	Industry 4.0, the Fourth Industrial Revolution, or 4IR, is the use of automation and IoT technology to create a more holistic and better-connected ecosystem, primarily for companies in the fields of manufacturing and supply chain management.
Intellectual property	WIPO lists intellectual property (IP) as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce."[7] Digital technologies have the potential to promote innovation, can be used as a means of distributing content that is IP, and can also be considered IP themselves, meaning they raise questions about the functioning of existing IP rules.
Intermediate liability	Intermediary liability describes the allocation of legal responsibility to digital content and service providers of all kinds of regulated categories of content. It involves defining the extent of legal liability digital platforms are subject to for the actions of their users. This is 'secondary' or 'indirect' liability as it does not relate directly to the intermediary's own conduct.
Internet economy	The Internet economy refers to economic activity being generated directly from the Internet. Generally, the Internet economy refers only to the economic activities directly associated with use of the Internet, including Internet companies such as ISPs, online content and advertising providers, developers of applications, e-commerce businesses, and data storage providers. (This is in contrast to the 'digital economy' – see above.)
Internet of Things	Internet of Things, or IoT, is the connecting of any electronic device to the Internet. The IoT is the online network of these devices, communicating with network users and with each other. For instance, a lightbulb could be turned on and off with a smartphone app using IoT technology.
Internet Protocol	IP or Internet Protocol is the set of rules governing the format of data sent via the internet or local network.

[7] WIPO (2021) What is Intellectual Property?, www.wipo.int/about-ip/en

Internet service provider (ISP)	A multimedia service provider who provides Internet access to the public; or a telecommunications service provider that provides customers connection to public Internet networks.[8]
Interoperability	The ability of technical systems, regulatory frameworks, and/or governance regimes to 'talk' to each other and thereby enable exchange.
Killer acquisition	A maneuver by a large incumbent, which uses its substantial cash reserves to buy-out competitors, or emerging companies that offer innovations with the potential to become competitors.
Legitimate public policy objectives	Legitimate public policy objectives or LPPOs are terms used in trade agreements that give economies scope to rebalance regulatory priorities within a certain remit. Facilitating trade growth tends to involve keeping regulation light-touch, and free trade agreements between economies usually reflect this. Nevertheless, within these agreements, there may be allowances for LPPOs that allow an economy greater maneuverability to refocus regulatory priorities, or to act in a manner that would otherwise run counter to the agreement but are determined to be necessary because of overriding domestic considerations. Ideally these are meant to be identifiable and only used in extra-ordinary circumstances.
Machine learning	Machine learning is a branch of artificial intelligence focusing on building up machine knowledge with human supervision, in which the machine learning tool improves its accuracy over time through exposure to more data and other inputs.
Network effects	Network effects or network externalities are when the utility derived from a good or service depends on the number of users of compatible products. They can be considered a demand-side economies of scale. For instance, online marketplaces such as Airbnb are of greater value to a user if there are already (or simultaneously) multiple thousands of other users.
Over-the-Top (OTT) service provider	Digital content distributed over the Internet that bypasses traditional communication delivery channels to reach end users, and that can potentially complement or supplant traditional telecoms and media services and, increasingly, a range of traditional industries, such as finance and education. Examples of such services include map services such as Google Maps, media providers such as Spotify, or education services such as Khan Academy. OTT business models are diverse and can include pay-to-access for specific content, as well as subscription- or advertising-based models. Many—if not most—services will increasingly be able to be delivered 'OTT' as the world continues to digitalize, in line with the maxim that 'everything that can become digital, will become digital'.[9]
Platforms	Platforms are sites or businesses that facilitate a relationship between users and third parties. This can include platforms that bring together providers and consumers offering material services (or 'sharing' of resources), such as Airbnb or Go-Jek, or access to a workforce, expertise, or labor tasks, such as AirTasker, and TaskRabbit, as well as platforms that provide access to money or capital, including crowdfunding sites such as Kickstarter and GoFundMe, and payment systems such as PayPal, Mastercard, Visa, and Bitcoin. Larger platforms (such as Apple's app store or Microsoft Windows) sometimes provide a foundation on which entire ecosystems are built.[10]

[8] Article 1.16, Ministerial Regulation 13/2019 on Telecommunication Services
[9] Landa Nano (2021) Nanographic Printing, www.landanano.com/nanography/nanography
[10] Ben Thompson (2019) A Framework for Regulating Competition on the Internet, https://stratechery.com/2019/a-framework-for-regulating-competition-on-the-internet

Quality of service (QoS)	The ITU defines Quality of service (QoS) as the "totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service". QoS standards can be included in licensing criteria for a service operator, and performance indicators often serve as a means for regulators to assess the performance of traffic on an operator's network and protect consumer interests accordingly.
Regulatory fragmentation	Regulatory fragmentation is the increasingly complex and complicated landscape of regional regulatory compliance requirements, as jurisdictions introduce new regulations that diverge from each other. This is exacerbated when digital regulatory requirements are incompatible across economies.
Smart cities	Smart cities are areas that adopt millions of sensors and IoT-networked devices to analyze and interpret phenomena. They can improve traffic management, logistics, and disaster response, among other issues, with immediate information and decision making.
Smart homes	Smart homes are homes in which networked devices can be managed or operated from any part of the home, usually through a smartphone. This heightens convenience for the user.
Subscription-video-on-demand (SVOD)	A type of video-on-demand (VOD) that gives users access to content at a monthly or annual fee. Examples include Netflix, Disney+ and Amazon's Prime Video.
Tokenization	Tokenization is the process of substituting sensitive data with a non-sensitive equivalent, referred to as a token. The token is a unique identification of symbols that maps back to all the sensitive data without compromising its security. Tokens are often used in payment processing.
User-generated-content provider (UGCP)	A host of online user-generated content, which may include social networking services; content aggregation services; Internet-based messaging services; and video-sharing services.
Video-on-demand (VOD)	Content that is either streamed or downloaded to a device, and can be consumed at the user's convenience, without any restriction to program schedule. The most common business models that incorporate video-on-demand are SVOD (subscription video-on-demand), TVOD (transactional video-on-demand or 'pay per view'), and AVOD (advertising-based video-on-demand).

Executive Summary

Digital technologies are rapidly transforming the world as we know it. Across the APEC region, mature and emerging economies are all making important digitalization strides. From online government services, smart cities, and digital identities to e-commerce, mobile banking, and electronic payments, the region's economies are prioritizing the development of data-powered economic models.

This **Primer on Economic Integration Issues Posed by the Digital Economy** aims to contribute to the thinking and efforts of APEC to accurately frame and therefore be better able to address the many cross-cutting challenges arising from the spread of the digital economy.

Emerging Policy Challenges

The cross-cutting nature of digitalization and digital transformation threatens to change the landscape for policymakers and regulators. As industries, markets, and pricing strategies are transformed, the traditional industry-specific approach to policy-setting is struggling to maintain effectiveness, while the traditional risk management regulatory approach is failing to deliver expected regulatory control and adequate consumer protection.

With the pandemic increasing reliance on the Internet, the critical role digital platforms play in creating access to goods and services, and the control they have over key distribution channels by acting as gateways to markets and users has become apparent. This is raising new challenges for regulators, including those related to competition, as well as security, privacy, and consumer protection. The governance, accountability, and transparency of digital platform businesses are, as a result, coming under greater scrutiny.

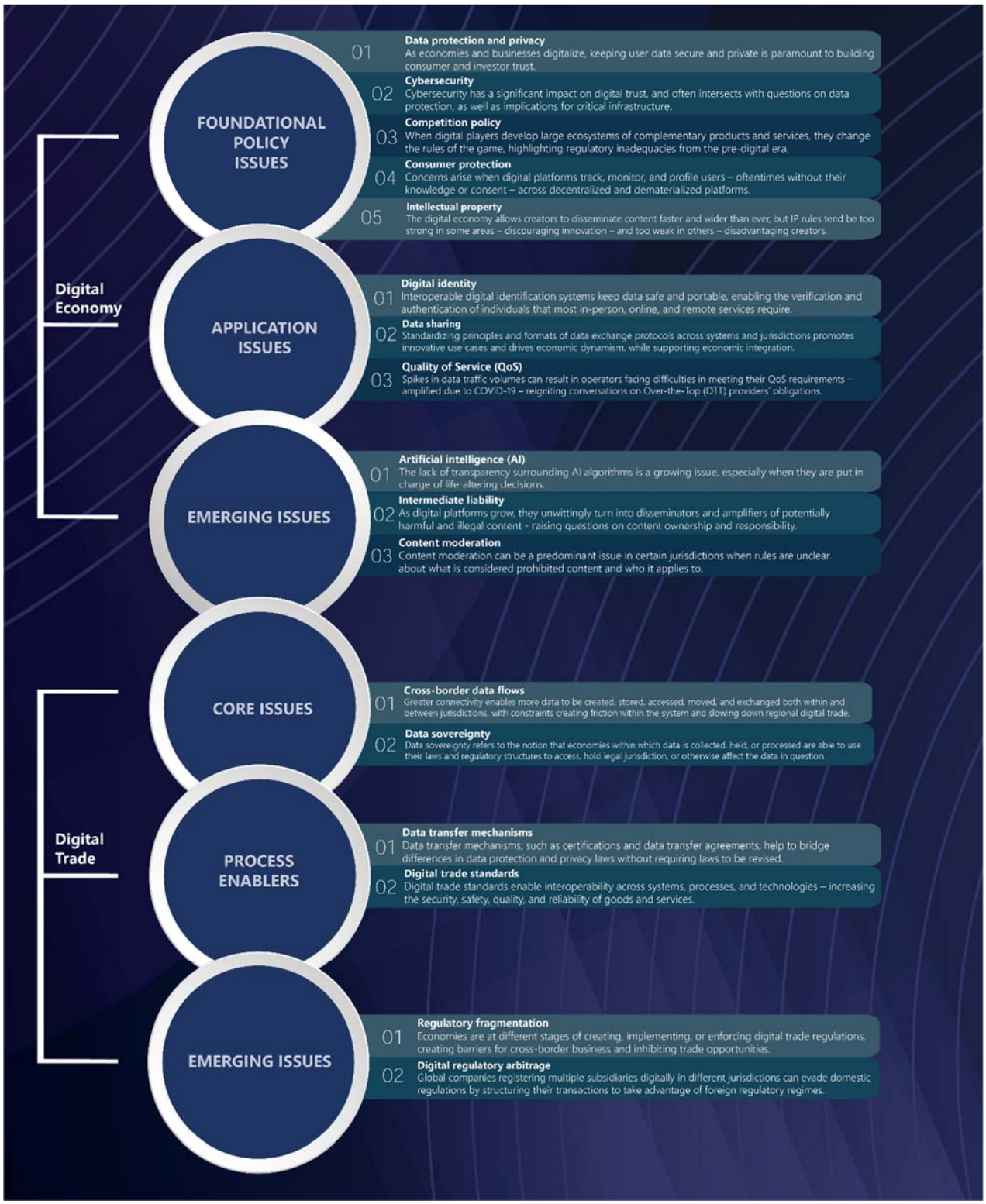
Digitalization requires examination of who should be regulating various aspects of digital economy and digital trade participation, who should be ensuring accountability and enforcement, and how those powers are to continue to work effectively. Increasingly, the intersection (and overlap in many cases) of regulatory responses—from competition policies to data governance requirements—are being examined and called into question. Navigating this intersection—and integration—between digital policies and regulation will be crucial in ensuring effective and fit-for-purpose policymaking.

For *trade*, the paradox confronting both policy makers and businesses is that even as digital consumption grows and digital economy initiatives mature, regulations *constraining* digital trade developments have accelerated, fragmenting the trade landscape—particularly in the APEC region.

Policies, and regulations are increasingly being developed 'by exceptionalism', i.e., targeting specific outlier or 'giant' companies rather than the economy drivers—in other words, targeting the players not the principles. These challenges are not unique to any one economy. In this context, it is important for APEC economies to understand the differences in drivers between the digital economy (domestic digital considerations) and digital trade (regional/global digital interconnections and value

chains). It is equally important that they identify the complexities emerging from the interconnected impact that result from digitalization of trade processes.

Figure 1: Overview of Key Digital Economy and Digital Trade Issues



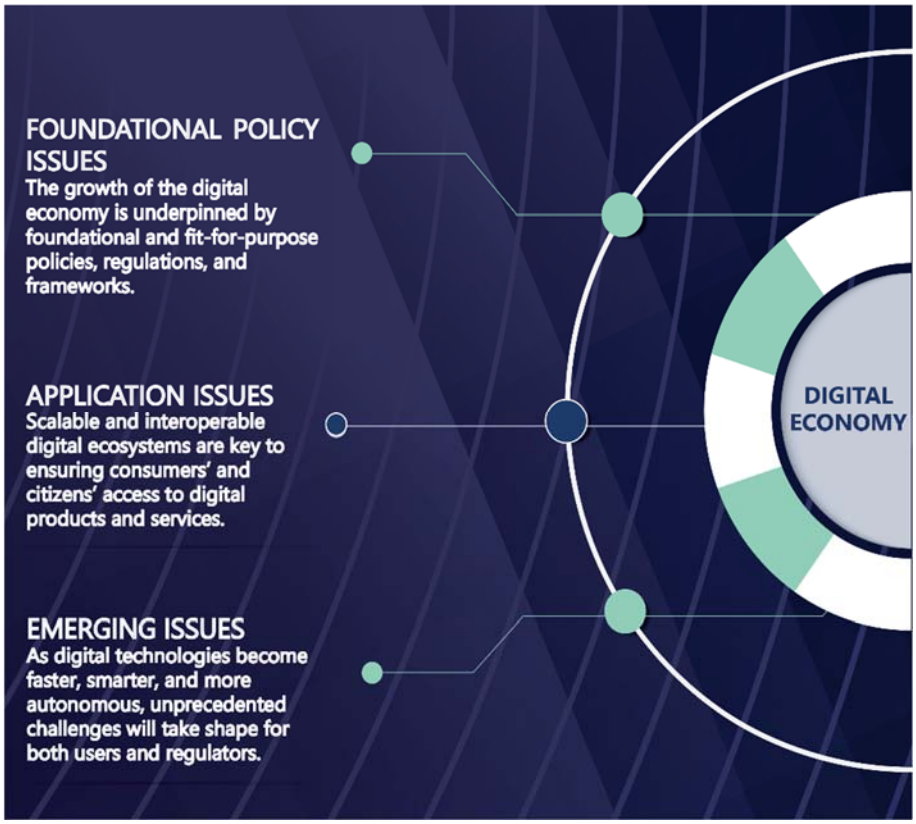
Source: Access Partnership (2021)

Digital Economy Issues

The cross-cutting nature of the Internet makes it a fundamental input and driver for all other sectors, such as financial services, healthcare, education, tourism, and hospitality and, as illustrated, in recent years through the sharing economy, transportation, housing, and many more. It is because of this pervasiveness that holistically understanding the impact and enabling the benefits of the digital economy has become so important, and so challenging.

At the heart of this challenge are three main types of issues: **i) Foundational policy challenges; ii) Issues of application;** and **iii) Emerging disruptors.** These issues are examined separately within the Primer so as to clarify and examine each in its own context; where possible the interconnections and interlinkages are also identified; it is the interplay of each of these issues that makes grappling with the emerging landscape so challenging. Policy—and trade policy, in particular—is inherently about compromise; a key objective of this Digital Primer is to help raise awareness of the complexity of issues that need to be considered in setting digital policy agendas.

Figure 2: Digital Economy Issues



Source: Access Partnership (2021)

Foundational Policy Challenges

When it comes to supporting the growth of the digital economy, clarity and certainty are the building blocks of conducive business and regulatory environments. Uncertain or ambiguous regulations can be just as inhibiting as restrictive or prohibitive ones. For example, a lack of regulatory clarity may limited direct foreign investment in e-commerce and other digital economy areas, or uncertainty around the interpretation and application of transactions and security regulations may curtail foreign investment and both intellectual and technology transfers.

Understanding the issues around data privacy, cybersecurity, competition, consumer protection, and intellectual property (IP) is crucial to developing effective and comprehensive foundational frameworks. This is important for APEC to address if the region is to boost digital economy and trade in a concerted and integrated manner.

- **Data protection and privacy**: As economies and businesses digitalize there is an increasing dependence on personal data for the delivery of economic goods and services. Advances in technology are facilitating more sophisticated use cases for personal data, requiring a balance to be found between ensuring strong protections while creating an enabling environment for data use.

  A key element when it comes to data protection and privacy is the need for requirements to be interoperable. This is especially true for sectoral privacy requirements (finance, health, education, etc.), which can sometimes be seen to not be aligned and thus not interact with one another—a trend we are seeing emerging both between and within economies.

- **Cybersecurity**: A key concern of organizations operating in the digital space is the risk of cyberattacks and information infrastructure breakdown. The risk of cyberattacks is increasing—rapidly—and will only continue to increase as the world grows interconnected. This is, and should be, of particular concern to the economic security of governments.

  Cybersecurity has a significant impact on digital trust, and often intersects with discussions regarding the safeguarding of personal data—while also having growing implications for businesses' and governments' vital infrastructure. This is especially important now that governments and private sector entities across the region are making use of ever larger amounts of personal information in the design and implementation of digital applications such as digital identities and artificial intelligence (AI) algorithms.

- **Competition policy**: Digital players have been expanding their services and platforms to develop large ecosystems of complementary products and services around their core offerings. The results have challenged economies to question whether competition laws and regulations from the pre-digital era remain fit-for-purpose and are able to effectively identify and curb market power in the digital economy.

  The interplay between competition law and digital policy (e.g., defining markets, assessing dominance applied to local presence requirements, data privacy provisions, consumer protection, and so on) has made close collaboration between different regulators crucial, as well close collaboration between competition authorities across jurisdictions.

- **Online consumer protection**: The ubiquity of digital platforms in consumers' daily lives, has grown hand-in-hand with the rising sensitivity of the data they collect (social interactions, buying habits, personal preferences and interests, locations, personal schedules, and plans, etc.). Users are constantly tracked, monitored, and profiled, oftentimes without adequate knowledge or consent.

  Algorithms used to process this information may often be seen to be a mystery for consumers, increasing consumer protection concerns. There is also concern over algorithmic profiling practices that may negatively affect consumers as well as competing businesses.

- **Intellectual property**: The digital economy has greatly improved the ability of creators, authors, businesses, and ISPs to disseminate goods, services, and content. This has highlighted that IP settings rules may no longer be fit-for-purpose, as they tend be too strong in some areas—discouraging innovation—and too weak in others—disadvantaging creators.

  Without the right mechanisms to regulate IP, international trade could be skewed as firms with strong IP rights prefer to export more often to economies with enforceable IP rights and policies. Supporting innovation and technology transfer should be key goals of IP regulation; therefore provisions that reflect those drivers will be required to ensure that both protections and flexibilities are adequate and appropriate for the digital age.

Issues of Application

In a world of increasingly globalized and digitalized economies, building secure and scalable digital ecosystems is key to ensuring consumers and citizens alike are able to access as many digital products and services as they need. An important example is the provision of social benefits, which are increasingly being delivered by governments and donor agencies through digital applications and platforms. As availability goes up and costs come down , having effective digital identity, data sharing, and Quality of Service (QoS) measures in place allows essential services, such as social protection, to gain in scale and scope, in capability, transparency, and thence efficiency.

- **Digital identity**: Economies are increasingly deploying digital identification systems to enable verification and authentication of individuals for a wide range of in-person, online, and remote transactions. For trade to take place, verifiable identifiers are important in all parts of the digital trade process across multiple parties where buyers, sellers, and service providers can prove and verify who they are and manage custody of goods.

  In terms of digital identity management, key areas of concern are security and privacy, particularly for biometric data. If a digital identification system is not sufficiently robust, it can jeopardize the personal data of citizens and residents. An associated issue, which will emerge with greater importance in the future, is interoperability with other identity systems. Economies will likely adopt different systems, but there are rewards to be reaped if the systems are interoperable and the data portable.

- **Data sharing**: Access to data—and the development of interoperable systems, platforms, and processes for the sharing of data—has implications across the public and private spheres, and in all economic sectors. More governments and businesses are adopting open

approaches to data sharing, with the aim to maximize access to promote innovative use cases and economic dynamism, while maintaining rigorous standards of trust.

While data sharing initiatives can have a significant effect on economic integration within individual economies and across regions, a major barrier is the lack of standardizing principles and formats for data exchange. Data formats or channels of exchange that are not interoperable or even readable across jurisdictions limit the degree to which separate jurisdictions are able to access and collaborate on data-related challenges using appropriately diverse and inclusive datasets.

- **Quality of service**: Quality of service (QoS) refers to characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service. Spikes in data traffic volumes and unanticipated changes in consumption patterns can result in operators facing difficulties in meeting their QoS obligations. This is a major barrier for governments, communities, and businesses who use the Internet for a range of digital activities.

  QoS can, and has been, used by various jurisdictions to address a set of issues, including net neutrality, digital competition, consumer choice, content moderation, and promotion of the digital economy—all on the basis of cost reallocation. There is an argument that a growing demand for high-bandwidth online services, such as subscription-video-on-demand (SVOD), have contributed to ISPs' and telcos' cost burden, and in some cases, impede on their ability to fulfil QoS requirements.

Emerging Disruptors

As digital technologies become faster, smarter, more autonomous, and more widely used, many new and unprecedented challenges will take shape for both users and regulators. From regulatory voids to the inadequacy of existing laws and policies, technological innovation consistently outpaces governments' ability to identify, understand, and regulate socio-technological phenomena. For example, regulators are just catching up to Fake News, but what will happen when AI algorithms are programed to create and spread disinformation? Likewise, Deep Fakes currently sit in a legal grey area, an ambiguity that may have major repercussions once the technology is used for nefarious purposes across platforms and jurisdictions.

- **Artificial intelligence**: AI technologies are being integrated into the digitalization of private and public sector enterprise across APEC member economies. Companies of all sizes, from entrepreneurs to MSMEs and major industrial enterprises, are using AI to improve competitiveness by optimizing business processes, automating tasks, and reducing costs. AI is enabling businesses to offer new products and services, while enabling governments to improve both their own efficiencies and their service offerings to citizens.

  A key factor underlying regulatory concerns is the lack of transparency surrounding AI algorithms, including how they collect and process data and how this translates into service provision from digital platforms. Without explanation about what factors led to the decision

and how it occurred, challenges arise when the AI is entrusted with life-altering decisions (i.e., social justice systems, hiring decisions, financial lending, etc.).

- **Intermediate liability**: Intermediary liability describes the allocation of legal responsibility to digital content and service providers of all kinds of regulated categories of content. Discussions on determining where liability rests and the extent of intermediary liability are focused on intermediary service providers who provide a mere conduit, caching, or hosting service (e.g., holding Facebook accountable for user-generated content published on their feed).

  Intermediary liability protections ('safe harbor') have been fundamental to the growth of the open Internet, providing a safety net that allows digital intermediaries to operate with the certainty that they will not be legally liable for storing, hosting, processing, or transmitting content, since the flipside of that is that digital intermediaries face higher legal risks that they will try to mitigate through early or unnecessary blocking of content or censorship. However, today these digital platforms are bigger, engaged in more activities, and offer more services—and have unwittingly turned into developers, disseminators, and amplifiers of potentially harmful and illegal content.

- **Content moderation**: Content moderation refers to the practice by online platforms to screen user-generated content and ensure that the published content does not violate rules and guidelines. Content moderation includes takedown demands, such as formal requests from governments to remove content that is deemed illegal, unlawful, or inappropriate.

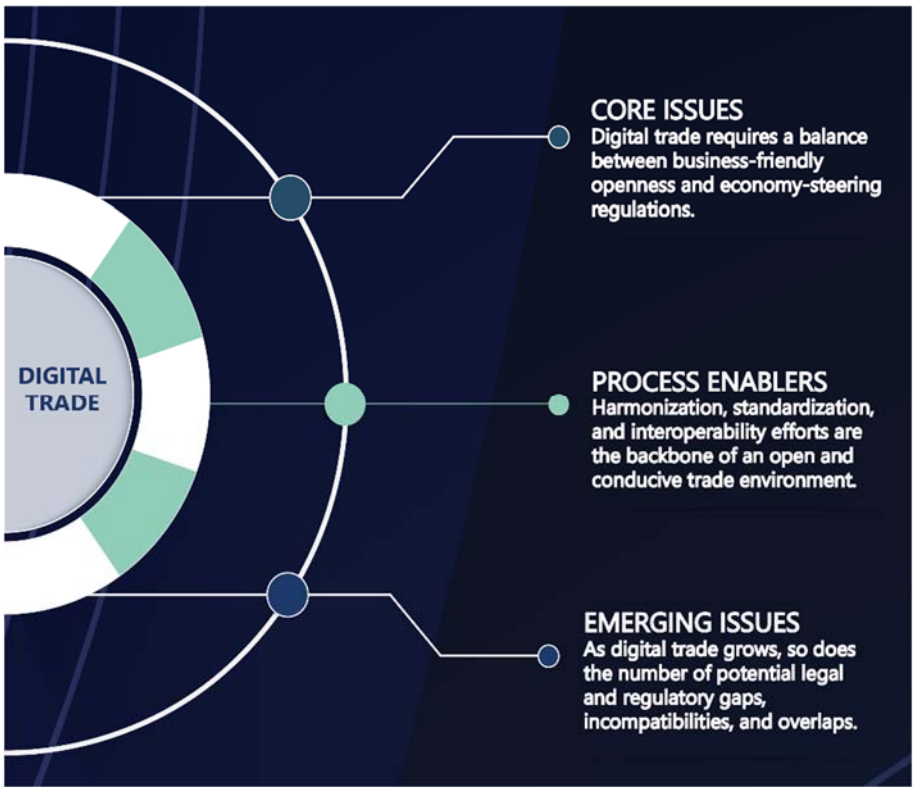
  Content moderation can be a predominant issue in certain jurisdictions when rules are unclear about *what* is considered prohibited content and *who* it applies to. A complex, global issue, content moderation requires principles-based measures, adaptable to technological developments, and balanced as under-moderation results in the spread of harm and abuse. Conversely, excessive content moderation may give rise to concerns around censorship, bias, and constraints on social interactions.

Digital Trade Issues

The globalization of the Internet and the ability to move data across borders underpins an increasing amount of economic activity and international trade. Digital technologies have transformed businesses and the way in which business is done, allowing any business to potentially reach overseas customers and sell products online. One of the major challenges currently in relation to digital trade is ensuring balance between openness, or facilitation of regional/global digital trade (e.g., limiting frictions within the system), and maintaining an economy's right to regulate for what are known as 'legitimate public policy objectives' (LPPOs).

At the heart of this challenge are three key areas to consider: **i) Issues that are core to trade flows; ii) Process enablers,** and **iii) Emerging digital trade fragmentation**. Again, these are examined separately within the Primer, but it is important to note that they function in close interconnectedness.

Figure 3: Digital Trade Issues



Source: Access Partnership (2021)

Issues Core to Trade Flows

Globalization and digitization have led to greater connectivity, which in turn has rapidly increased the quantities of data being created, stored, accessed, moved, and exchanged both within and between jurisdictions. This increases the chances of new risks, new twists on old risks, as well as unintended consequences to take shape. Systems can fail and undermine market stability; machines can make decisions with harmful, unintended consequences; and data—the lifeblood of the digital world—can be manipulated, misused, stolen or, because of its sheer volume and complexity, be used to disguise criminal behavior.

- **Cross-border data flows**: Cross-border data flows refer to the movement of data across domestic borders and are key to any form of digital trade. For regional digital trade to flourish, cross-border data flows need to be facilitated at the regional level. Cross-border data flows underpinning digital trade include digital commerce and electronic- and mobile-money transfers, the exchange of health records or validation of identity between jurisdictions, the access of non-local websites and content (both from traditional broadcast and OTT-delivered social media), and many more.

  Measures put in place to slow down or restrict the flow of data (such as data localization measures) may increase barriers to market entry and undermine businesses' ability to expand to overseas markets. Further, limitations to data flows have a much wider impact to

an economy through reduced consumer choice and access, and repercussions on broader economic growth and innovation. Regulators need to strike a delicate balance between regimes which adequately address data transfer issues and promoting a business-friendly environment which still enables the flow of data. Different challenges emerge across different uses of data within emergent technologies.

- **Data sovereignty**: Data sovereignty is premised on the idea that economies within which data is collected, held, or processed, are able to use their laws and regulatory structures to access or otherwise affect the data in question. A principle of data sovereignty asserts that data held within an economy is subject to that economy's laws and regulatory structures. This imposes an additional layer of regulatory obligation onto data owners and processors, beyond those imposed in the context of corporate data governance.

  Various economies are taking different stances on both the issue of data sovereignty and the underlying principle. The rise in adoption and application of the concept is largely playing out along two tracks: i) economies perceive security vulnerabilities resulting from the greater exposure of domestically produced data to data owners or processors in other jurisdictions; and ii) there is an elevated understanding of the economic potential associated with *control* over data resources.

Process enablers

Just as there are emerging social, technological, commercial, or government policy-related developments that can imperil digital trade, there are measures and approaches that facilitate, encourage, and enable its growth. In the context of regional integration of digital economies, regional harmonization, standardization, and interoperability efforts will go a long way in setting the foundations for an open and conducive trade environment for both businesses and governments.

- **Data transfer mechanisms**: For information to be transferred across borders securely, economies must recognize each other's data privacy and protection regimes. Data transfer mechanisms, such as certifications and data transfer agreements, help bridge differences in data protection and privacy laws without requiring laws to be revised. In recent years, mechanisms that seek to facilitate interoperability across data protection/privacy regimes have emerged, providing an avenue to ease compliance costs and business uncertainty, allowing innovative digital offerings to penetrate local markets, and at the same time ensuring the safe and secure flow of data.

  When regional or multilateral organizations develop certification programs, they can mitigate uncertainty with regards to otherwise divergent regulatory regimes between different member economies. For example, the APEC Cross-Border Privacy Rules (CBPR) system provides a mechanism that enables trust and data flows amongst participants. This occurs even in the absence of governments formally recognizing that another jurisdiction has equivalent protection.

- **Digital trade standards**: The use of standards can enable a high benchmark for security, safety, quality, and reliability of goods and services being delivered into a market. In turn,

the implementation of standards increases the interoperability of the processes, technologies, or methods standardized across the range of producers, suppliers, and consumers.

The encompassed activities considered to be within the scope of digital trade is only expected to increase as new technologies such as the Internet-of-Things (IoT), AI, 5G mobile communications, and developments such as blockchain gain traction, and both economies and communities become more interconnected. For IoT and 5G to work at scale—fridges, toasters, hair irons, ice machines, and air conditioners need to be standardized in line with the communications protocols. This is what is currently playing out for example in autonomous vehicles and smart homes.

Emerging digital trade fragmentation

There are a variety (and rapidly increasing number) of different *types* of regulations relevant to the digital economy (e.g., data protection and privacy, cybersecurity, online consumer protection, and various sectoral regulatory applications, as well as emerging data sharing and AI requirements), with many economies at vastly different stages of creating, implementing, or enforcing these regulations. As regional and global digital trade advances, so does the number of potential legal and regulatory gaps; from incompatible rules to overlapping roles, it will become increasingly difficult to fairly and accurately arbitrate when contentions arise.

- **Regulatory fragmentation**: Regulatory fragmentation creates barriers not only for cross-border business—increasing compliance costs—but also generates a 'drag' on the potential economies of scale and scope available to an economy (and the businesses within) resulting in missed opportunities to trade. The extent of regulatory fragmentation is very likely to increase due to ongoing pressures to speed up economic recovery from COVID-19 (with economies focusing on domestic markets over cross-border trade), and inconsistent implementation of international standards.

  Seizing the opportunity presented by digital trade, and realizing its potential for APEC's economic growth, will depend on the development and implementation of harmonized digital trade rules. Trade rules help remove a host of barriers impeding trade such as cross-border data flow restrictions, localization requirements, tariffs and quotas on ICT equipment, domestic and local standards that deviate from international standards, and lack of access to effective dispute resolution mechanisms. They also promote cooperation among economies by encouraging individual economies to move away from putting in place rules that are protectionist in nature, and hinder the growth of digital trade.

- **Digital regulatory arbitrage**: Regulatory arbitrage occurs where different jurisdictions create different sets of laws and regulations, and persons or corporate entities that operate across borders have the opportunity to take advantage of whichever offers the greater benefits (for example in taxation, in labor laws, in health and safety standards, or in consumer protection). *Digital* regulatory arbitrage has been further compounded by various economies seeking to establish the global regulatory precedence of *their* requirements through extraterritorial application.

The Internet has made regulatory arbitrage easier to manage because global companies (alternatively referred to as international, multinational, or transnational companies) are able to create multiple subsidiaries which can be registered digitally in different jurisdictions. This is a major driver behind global value chains (GVC). These companies can then use transfer pricing to shift taxable revenues from one jurisdiction to another.

Cross-Cutting Issues

The issues described above are not taking place in a vacuum. For several years now, APEC member economies have been examining them for their multi-sectoral, inter-related impact on key aspects of digital economy and digital trade. Five areas stand out in this regard: i**) Development; ii) Inclusivity; iii) Equality; iv) Sustainability;** and **v) Entrepreneurship.**

- **Digital and Development**: Although the extent of digitalization is likely to be far greater in high-income economies, the success of digitalization is not confined to those economies. This is because going digital is not only about the advantages of technological development, but also about the innovative use of the digital technologies that are available to an economy. The reality is that most of these are available either over the Internet as applications or from many vendors competing for global markets.

  A prerequisite is an electricity supply, which means that the foundations of digitization require an adequate infrastructure of power lines and broadband telecommunications. Lower-income economies therefore need to plan strategically these complementary developments that will spur their economies to move more rapidly up the value chain of production, from food scarcity to food security, from absolute poverty to sustainable living standards, from a lack of access to education to both online and offline schooling for children and lifelong learning for adults to adapt to economic and social changes, and from a lack of access to health services to improved welfare provisions and health education.

- **Driving Inclusivity**: The benefits of digitalization can be especially important for women and marginalized communities by bringing connectivity to everyone. Going digital significantly reduces the cost of providing services, expands the reach of jobs and services and when, for example, applied to banking and finance, enables even the poorest of families an ability to receive and to send payments, either as remittances from family members working overseas, or as welfare payments from government, or as income from different sources.

  Several APEC projects on the economic empowerment of Indigenous Peoples are increasingly demonstrating that differing and additional policy issues will come into play in this context. In particular, Indigenous Peoples have expressed a strong interest in the types of policy approaches that are adopted in areas such as Indigenous data governance and the treatment of traditional knowledge online—particularly as this relates to the intersection of intellectual property and digital policies.

- **Closing the Digital Divide**: Digital—and digital trade—is a potentially great leveler for diversity, disability, and minorities. Although prior to the pandemic there were warnings of an increasing gap between the haves (e.g., digital access) and the have nots, this has been

exacerbated by the COVID-19 pandemic, with women and minorities being disproportionately impacted.

Digital should provide the channel for addressing this trend at a time when it is crucially needed for economic recovery and social stability. This raises an enormous opportunity for many developing economies to raise their productiveness by the simple measure of bringing greater access to women who are too often denied the opportunities to be fully involved in the economy or in many aspects of society.

- **Green Digitalization and Sustainability**: Digitalization is offering new ways to create environmentally sustainable 'green' growth. The examples are endless and growing by the day. They range, at the citizen and business-user end, from ways to monitor and reduce energy consumption in 'smart buildings', the replacement of oil and gas driven vehicles with electric or hydrogen-fueled vehicles controlled by digital operating systems, to carbon-reducing industrial processes that replace electrical-mechanical with digitally-controlled production process and SVCs where all processes from packing and trucking to customs and storage are digitally managed, to the greatest challenge of all, the production of power by renewable sources of energy.

  Sustainability involves more than environmental protection, although that is the most pressing need. It also involves financial sustainability. The financial community is becoming increasingly aware of the danger of 'greenwashing' when approached to fund investments in environmental, social, and governance (ESG) projects and is developing standards by which to seriously judge their outcomes, and mechanisms to reduce the risk-to-return ratio for private investors, especially in developing economies, through schemes of 'blended finance' which combine public and overseas development assistance funding (ODA) with private investments.

- **Digitalization of Businesses Big and Small**: Digitalization of businesses all along the SVC, from small farms through to manufacturers to end-user supermarkets is available to most enterprises, big or small. Digital technologies are driven by software algorithms processed through microprocessors in their electronics. It is normal today to buy business equipment of all types fully digitized, and especially for small businesses the widespread digitalization of smart mobile networks offers enormous flexibility to transact business, including almost simultaneous payments where such systems have been introduced.

  The ability of small businesses to reach new markets supports economic growth everywhere; as demonstrated by SMEs' contribution to GDP ranging from 40% to 60% in most APEC economies. SMEs also employ over half the workforce across APEC. Further, individuals participate in globalization directly by using digital platforms to access information, to learn, find work, showcase their talent, and build social networks. These individuals gain social benefits from e-government services, are financially included, make purchases online, benefit from online education, or are assisted by remote medical facilities.

Primer Overview

Digital technologies have transformed industries and businesses, and changed the roles people, products, and platforms play in key economic sectors, including finance, transport, tourism, logistics, healthcare, education, agriculture, and many others. Digital platforms have changed the economics of doing business across borders, bringing down the cost of international interactions and transactions. They create markets and user communities on a global scale, providing businesses with a huge base of potential customers and effective ways to reach them.

The cross-cutting nature of digitalization and digital transformation threatens to change the landscape for policymakers and regulators. As industries, markets, and pricing strategies are transformed, the traditional industry-specific approach to policy setting will increasingly fail to enable expected economic growth and social development outcomes. Even more challenging is the job confronting the regulator, with the traditional risk management-oriented approach failing to deliver expected regulatory control or provide adequate consumer protection.

This **Primer on Economic Integration Issues Posed by the Digital Economy** aims to contribute to the thinking and efforts of APEC to accurately frame and therefore be better able to address the many cross-cutting challenges arising from the spread of the digital economy.

Objective

The Primer identifies, explains, and then connects the various factors required for the acceleration of digital trade through regional coordination and the utilization of digital technology and tools to enhance and promote regional economic integration.

It also highlights factors that APEC member economies can consider to maximize the benefits and the enormous growth potential of digital trade, including:

- **Coordinated regional approach:** Domestic policy and practices that address, and enable trade to be conducted as a region; and
- **Interoperability:** Member economies' technical systems and regulatory and governance frameworks are able to 'talk' to each other.

Regulation and administrative procedures at the domestic member economy level (e.g., policies and practices that are focused on driving and developing the *digital economy*) may constrain and impede effective and efficient trade across the region (e.g., facilitation of regional/global *digital trade*, interconnections and value chains)—and in turn may affect the quality and efficiency of any individual domestic digital economy.

The promotion of a coordinated and coherent regional approach will indeed ensure member economies consider digitalization and the development of the *digital economy* from the objective of fewer barriers to trade—leading to lower costs, more transactions, and greater economic benefit.

One of the major challenges currently in relation to digital trade is ensuring balance between openness, or facilitation of regional/global digital trade (e.g., limiting frictions within the system), and maintaining an economy's right to regulate for what are known as 'legitimate public policy objectives' (LPPOs). Consistent with the stated purpose, this Primer does not seek to prescribe how that balance should be struck, but sets out some of the issues to assist economies in considering how and when to provide meaningful and effective protections in a way that does not 'swallow the rule'—i.e., undermine the benefits of openness.

Ultimately, there may need to be a parallel process to the one that has occurred with treatment of exceptions in trade agreements—where similar issues arise and where counter-balancing principles of not using unjustified discrimination, not applying disguised restrictions on trade, and limiting any restrictions to that which is necessary to achieve the legitimate public policy objective—have proved effective in striking an acceptable balance.

Trade, by definition, requires interaction across not just borders, but across disparate systems; digital trade, therefore requires not just 'interoperability', but the emergence and establishment of data transfer mechanisms able to *translate* between different domestic regimes, along with the need to simultaneously address issues such as accountability and enforcement. Further enabling or enhancing this regional (or global) trading system is the recognition, acceptance and use of internationally accepted digital trade standards, while recognizing the impact of cross-cutting issues such as security and safety, privacy, competition and consumer protection, sustainability, and universal access and opportunity.

Such awareness and understanding will serve to support APEC digital trade by ensuring:

1. **Interoperability** in digital systems for transparency, simplicity, and compliance;
2. **Mutual compatibility** in products, components and services, especially where digital developments have created new products, components or services, or introduced elements of risk;
3. **Flexibility** and promptness in responding to new challenges or changes in such processes that will inevitably occur as digital economy and digital trade frameworks continue to adapt and change; and
4. **Consistency** in the quality of goods or services, with appropriate safety and security safeguards.

The Primer does not claim to address all digital economy policy issues faced by member economies; it focuses on the major ones that require immediate and holistic attention as economic markets and environments rapidly evolve.

Approach

This Primer provides an illustrative reference on a core selection of digital issues in three interconnected and, at times, overlapping sections:

- **Section 1**: Examines key definitions and overarching frameworks currently used, highlighting some of the main cross-cutting issues underpinning digital economy and digital trade development.
- **Section 2**: Focuses on those issues central to digital economy growth, transformation, and opportunity.
- **Section 3**: Explores the dynamics and challenges related to digital trade and digital supply and value chains.

The following table summarizes the issues to be examined within the Primer, focusing on economic integration issues that member economies and the region are facing.[11]

Table 1: Primer Issues

Digital Economy	Digital Trade
Foundational policy issues • Data protection and privacy • Cybersecurity • Competition policy • Consumer protection • Intellectual property (IP)	Core issues • Cross-border data flows • Data sovereignty
Application issues • Digital identity • Data sharing • Quality of Service (QoS)	Process enablers • Data transfer mechanisms • Digital trade standards
Emerging issues • Artificial Intelligence (AI) • Intermediate liability • Content moderation	Emerging issues • Regulatory fragmentation • Digital regulatory arbitrage

[11] Areas such as connectivity (including infrastructure rollout), trade facilitation measures (including e-invoicing, digital signatures, single windows, etc.), and skills (including the need to re- and upskill to enable digital transformation) continue to be extensively addressed at the member economy level, and through a number of APEC initiatives.

Each module will provide an initial and indicative understanding by capturing the current array of issues in the following format:

1. **What is the issue:** brief introduction to the policy and/or regulatory area/issue in discussion;
2. **Why is it/will it be an issue**: for member economies and the region;
3. **Considerations/challenges:** identification of approaches that can lead to frictions and either have or may result in unintended consequences that regulators and/or market participants can face;
4. **Emerging practices:** example(s) of what economies are putting in place and some of the lessons being learnt; and
5. **Key takeaways:** from the issue, and emerging solutions and proposals that better suit the realities of digital.

1. Key Concepts and Issues

It is crucial to define and understand the key concepts and issues around domestic digital economy developments, and how they interact with and facilitate transactions between economies—i.e., cross-border digital trade. Some important terms are often ambiguous, and how they are used can change both over time and in different context.

The Primer seeks to provide foundational understanding and awareness of these terms, and in doing so, provide the relevant context in understanding how each of the identified issues are framed and interpreted.

1.1 Key Concepts

1.1.1 Digital Economy

Definition

A digital economy is not a 'thing' that can be observed, but rather a concept that can be described in many different ways according to which focus is considered the most important. The closest a description might come to a definition would be an account of what 'digital' means and the mechanisms by which each transaction in an economy is accompanied by a flow of digital data.

While the 'Internet economy' and 'digital economy' are at times used interchangeably, they point to how narrow or how broad the concept can be scoped.

The Internet economy refers to economic activity being generated directly from the Internet. Generally, the Internet economy refers only to the economic activities directly associated with the use of the Internet, including Internet companies such as ISPs, online content and advertising providers, developers of applications, e-commerce businesses, data storage providers, and so on. However, this approach also risks missing significant value and impact. When, for example, is an e-commerce company an *e-commerce company*, and not simply a retailer (a flower seller, bookstore) or service provider (consultancy, law firm) using the Internet to develop, market, and extend their existing business?

Defining the Internet economy as being the contribution to GDP directly derived from Internet-based or -related companies provides a framework for capturing and measuring economic impact (e.g., the production value and employment due to ISPs and e-commerce companies), as well as for regulating the Internet (e.g., limit or promote Internet access, protect consumers, or capture surplus value).

The digital economy encompasses all sectors of the economy that rely upon or use Internet Protocol (IP)-enabled networks and platforms as part of the embedded infrastructure of the society. In fully digitalized economies, this includes all major sectors of the economy and society. Achieving the transition to a digital economy requires both the growth of an ecosystem that will support new

entrants into the Internet economy, and the promotion of backward linkages from the Internet economy into the traditional economy.

There comes an inflexion point when the quantitative adoption of digitalization takes a quantum leap to become the 'new norm' or a paradigm shift across the economy and society, such as with the growth of e-commerce, business platforms, and social media and this is often termed a *digital transformation*. Technologies and applications, available on smart devices and websites, such as Artificial intelligence (AI) and Big Data, which is digital data from multiple sources, increasingly become the drivers of policymaking and business decisions.

Drivers

The digital economy is a global phenomenon and one of the most important drivers of economic growth and competitiveness today. Whether for entrepreneurs running small- or medium-sized businesses or executives of large corporations, the pervasiveness of the digital economy is felt across all spectrums of industry. However, for most businesses, especially in developing economies, the ability to take full advantage of the opportunities created by the digital economy is still, all too often, out of reach.

Progression towards a digital economy is built upon two key network issues:

1. **Interconnectivity of networks** means that digital traffic can travel across and between networks. This enables economies of scale as the fixed costs of infrastructure rollout are spread across a greater level of output bringing about a fall in unit costs.
2. **Interoperability of operating platforms** means that digital traffic can run effectively across different types of networks (e.g., from telecoms to banking to educational to health networks and so on). This enables economies of scope, as fixed costs are spread across a wider range of output of different products and services.[12]

The latter is particularly important in creating the conditions for innovation, and new products and services to emerge. Economies of scale and of scope create a virtuous cycle by driving down costs, increasing user choice of products and services and, in turn, stimulating market innovation and economic growth. An obvious and prominent example has been the rise of social media, and its use across a multitude of economic and social purposes, such as e-commerce and e-government.

Achieving the transition to a fully functioning digital economy requires the growth of an ecosystem supporting new entrants and the promotion of linkages back into the traditional economy (e.g., agriculture and aquaculture, manufacturing production and services, distribution, and consumption). Fully realizing the potential of a digital society means recognizing two further issues: i) promoting and assessing economic impact goes well beyond simple GDP growth to encompass such factors as

[12] TRPC, ISOC (2014) Unleashing the potential of the internet for ASEAN economies, www.internetsociety.org/sites/default/files/ASEAN_ISOC_Digital_Economy_Report_Full_0.pdf

employment, productivity, etc.; and ii) the impact of digitization and interoperability is as much on overall social development as on economic growth.

A key challenge for policymakers is that while they have some influence over the development of their own digital economy, they are far less able to determine digital trade, especially in a world of seamless data transfers. Another challenge is the need for timeliness given the speed of change and impact of digital, and the need for a set of common frameworks. However, the need for greater responsiveness is itself opening the door to new approaches such as cross-sectoral initiatives and overarching frameworks.

The inherently transnational, cross-border nature of digitization and data flow means that regional consistency and cooperation can have a disproportionate impact on digital society development. Constraints on e-commerce transactions or mobile money transfers such as international remittance will not only curtail the flow of digital goods and services, and the inflow of funds., For smaller or emerging economies these constraints result in less interest from foreign participants—often the leaders in the sector—and a far slower transfer of expertise and skills, as well as a dampening of potential demand for the ancillary goods and services that build in the ecosystem around new innovative sectors and developer communities.

Given its importance for a digital economy, the Internet, and policies towards it, should not be regarded in isolation, as a sector within itself. Rather, its cross-cutting role should be the focus of attention. This comes out most clearly if networks not only interconnect, but their platforms and operating systems are interoperable, allowing apps and content to be used across multiple devices. This is the essence of a connected digital economy. Applying these principles of 'any-to-any' connectivity to areas such as e-health, e-education, m-commerce, and e-transactions is the road to a fully digital society.

1.1.2 Digital Trade

Definition

'Digital trade' is a relatively young and developing aspect of trade and many of its broader implications are not yet fully understood. This can in part be explained by the absence of a common understanding and measure of the impact of digitalization, as well as by the need to use a narrower definition of digital trade to identify, size, and sometimes determine public policy.

Digital technologies help expand existing markets *and* create new trade possibilities. In both cases, they contribute to the creation of new jobs, to increased labor opportunities and wages, and to a higher standard of living. For instance, the OECD's framework for digital trade is being developed

around the idea that digital technology is changing the speed, scope, and scale of trading channels while increasing the value of trade.[13]

The term 'digital trade' is sometimes used interchangeably with that of 'e-commerce', or other similar proxies. Digital trade in fact has far broader scope, encompassing the increasing digitalization undergirding most facets of trade: the use of digital technologies in supply chains and logistics; the invention of new, commercially valuable communications and market access channels; and the value of the data that is created, transferred, and processed—not least because the data itself is increasingly both an asset input into the supply chain process and is being traded as its own discernible commodity.

We identify four components of digital trade, which are not mutually exclusive and may in combination be a part of a single transaction, product, or service:

1. **Digital goods and services**: We describe this component to include:
    a. Digital goods are those that are stored, delivered, and used in electronic format. Examples of digital goods include e-publishing, music files, software, digital images, web site templates, manuals in electronic format, and any item which can be electronically stored in a file or multiple files. It can also include digital content which can be news, as well as the intellectual property (IP) rights of the content.
    b. Digital services require digital technology (which is often subject to intellectual property rights and licenses) for access and consumption. Examples include cloud computing services, digital video telephony services.[14]
    c. Digital trade can also include trade in intellectual property independent of trade in goods and services.
2. **Digital delivery (full or partial) of tangible goods and services:** The delivery and/or purchase of a product can be online, such as via a digital platform. However, the good or service may be consumed physically.[15]
3. **Digital enablers of trade** which include the hard and soft infrastructure (cables and wires, platforms and devices, through to regulations) that protect data and IT systems such as digital logistics systems, goods tracking, privacy and cybersecurity, all of which support digital trade transactions. We consider four key digital enablers that increase the capabilities and reliability of the systems and technology, that can be deployed to support all forms of digital trade:
    a. **Infrastructure**: Provides the means to access services, content and communications. This includes the virtual networks and platforms that can facilitate the movement of goods and services.

[13] Javier López González and Marie-Agnes Jouanjean (2017) Digital Trade: Developing a Framework for Analysis, http://dx.doi.org/10.1787/524c8c83-en
[14] Javier López González and Marie-Agnes Jouanjean (2017) Digital Trade: Developing a Framework for Analysis, http://dx.doi.org/10.1787/524c8c83-en
[15] Javier López González and Marie-Agnes Jouanjean (2017) Digital Trade: Developing a Framework for Analysis, http://dx.doi.org/10.1787/524c8c83-en

   b. **Soft infrastructure**: Provides the ability to validate the parties to a transaction and audit and authenticate those transactions in all parts of the digital trade process (e.g., digital identities)
   c. **Transactions**: Whether on smartphones or online, digital payments can increase efficiency, speed, transparency, and security by lowering the cost of access and participation, thereby extending inclusion, as well as by increasing accountability and tracking and reducing the scope for fraud.
   d. **Trust and safety**: Refers to a broad range of protection services and support (privacy, piracy and theft, censorship, cybersecurity). Such measures are essential in developing user confidence and assurance.
4. **Emerging digital technologies:** New technologies that are currently developing or will be developed over the next five to fifteen years, and have the potential to transform aspects of trade practice and process. Examples include 5G, blockchain technology, AI IoT, 3D-printing, and tokenization.

Drivers

Digital trade will continue being a key driver of international trade—with global trade in goods declining as an overall percentage of trade, and trade in services plateauing. Looking ahead, the digital sector is expected to contribute 2.3% of total trade in the Asia Pacific region in 2021, with 43% of the increase in trade coming from the region by 2025.[16]

The paradox has been that even as digital consumption grows and digital economy initiatives mature along with this growth, regulations constraining digital trade developments have accelerated, fragmenting the digital trade landscape—particularly in this region. This has resulted in a rapid proliferation of several 'digital' drivers and concerns—which are all interlinked, interconnected, cross-cutting, and co-dependent.

For example, how do we consider and ensure safe and secure access to data from a privacy perspective versus a competition policy perspective? What international standards are we leveraging to hold organizations accountable for holding that data safe and secure? How do we enable data transfers? How do we ensure data can be shared to ensure access and continued innovation, and used in crucial digital applications and processes, such as digital identity systems? And how then do emerging technologies, such as artificial intelligence (AI) change the data landscape?

Ultimately, there may need to be a parallel process to the one that has occurred with treatment of exceptions in trade agreements—where similar issues arise and where counter-balancing principles of not using unjustified discrimination, not applying disguised restrictions on trade, and limiting any restrictions to that which is necessary to achieve the legitimate public policy objective—have proved effective in striking an acceptable balance.

[16] Statista (2021) Forecasted impact of digital sector growth on trade APAC 2021-2025, by subregion, www.statista.com/statistics/1221293/apac-digital-sector-impact-on-trade-by-subregion

Trade, by definition, requires interaction across not just borders, but across disparate systems; digital trade, therefore requires not just 'interoperability', but the emergence and establishment of data transfer mechanisms able to *translate* between different domestic regimes, along with the need to simultaneously address issues such as accountability and enforcement.

Further enabling or enhancing this regional (or global) trading system is the recognition, acceptance and use of internationally accepted digital trade standards, while recognizing the impact of cross-cutting issues such as security and safety, privacy, competition and consumer protection, sustainability, and universal access and opportunity.

1.2 Cross-Cutting Issues

In order to understand how cross-cutting issues should be *understood and placed* within context, we need to first understand how they are being *viewed* in context—from how we are taking into consideration different levels of capacity and resources for developing economies; how we should be addressing diversity and inclusion, including addressing the gender digital divide; how sustainability and other mega trends are impacting; and how we are taking into consideration businesses of all sizes, including SMEs and MSMEs.

1.2.1 Digital and Development

Although the extent of digitalization is likely to be far greater in high-income economies, the success of digitalization is not confined to those economies. This is because going digital is not only about the advantages of technological development, but also about the innovative use of the digital technologies that are available to an economy.

The reality is that most of these are available either over the Internet as applications or from many vendors competing for global markets. For example, products that are part of the Internet-of-Things (IoT) and the use is sensors that can be attached to machines to enable them to be connected by the Internet to control panels, to dashboards, to other machines, to end users.

A prerequisite is an electricity supply, which means that the foundations of digitization require an adequate infrastructure of power lines and broadband telecommunications. Lower-income economies therefore need to plan strategically these complementary developments that will spur their economies to move more rapidly up the value chain of production, from food scarcity to food security, from absolute poverty to sustainable living standards, from a lack of access to education to both online and offline schooling for children and lifelong learning for adults to adapt to economic and social changes, and from a lack of access to health services to improved welfare provisions and health education.

1.2.2 Driving Inclusivity

The benefits of digitalization can be especially important for women and marginalized communities by bringing connectivity to everyone. Going digital significantly reduces the cost of providing services, expands the reach of jobs and services and when, for example, applied to banking and

finance, enables even the poorest of families an ability to receive and to send payments, either as remittances from family members working overseas, or as welfare payments from government, or as income from different sources.

Several APEC projects on the economic empowerment of Indigenous Peoples are increasingly demonstrating that differing and additional policy issues will come into play in this context. In particular, Indigenous Peoples have expressed a strong interest in the types of policy approaches that are adopted in areas such as Indigenous data governance and the treatment of traditional knowledge online—particularly as this relates to the intersection of intellectual property and digital policies.

For example, the Māori Data Sovereignty Network aims to raise awareness on the fact that Māori data could/should be subject to Māori governance.[17] As New Zealand's Integrated Data Infrastructure (IDI) initiative expands, the Māori Data Sovereignty Network looks to build a robust Māori data governance partnership that is representative, enabling, and provides clear lines of accountability back to Māori/Iwi. In the United States, the Native Nations Institute calls for a "decolonization of data", calling for governments, industries, and organizations to recognize and respect Indigenous data sovereignty.[18]

Further work is needed to flesh out such issues as a contribution to APEC's overall work program on Indigenous economic empowerment.

1.2.3 Closing the Digital Divide

Digital—and digital trade—is a potentially great leveler for diversity, disability, and minorities. Although prior to the pandemic there were warnings of an increasing gap between the haves (e.g., digital access) and the have nots, this has been exacerbated by the pandemic,[19] with women[20] and minorities[21] being disproportionately impacted.

Working online from home during lockdowns, buying online, texting and video calling, online schooling, online medical consultations, the use of mobile communications to track and trace pandemic outbreaks, a growing market for social media news and information services and streamed

[17] Māori Data Sovereignty Network (2021) Ngā mihi ki a koutou katoa, www.temanararaunga.maori.nz
[18] Native Nations Institute (2020) Indigenous data sovereignty in the United States, https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/5b297686f950b7690cf0f9a9/1529443976962/Policy+Brief+Indigenous+Data+Sovereignty+in+the+United+States+V0.3+copy.pdf
[19] World Economic Forum (2020) COVID-19 is increasing multiple kinds of inequality. Here's what we can do about it, www.weforum.org/agenda/2020/10/covid-19-is-increasing-multiple-kinds-of-inequality-here-s-what-we-can-do-about-it
[20] Washington Post (2021) How the pandemic set back women's progress in the global workforce, www.washingtonpost.com/world/interactive/2021/coronavirus-women-work
[21] UN Human Rights Council (2021) The magnitude and scope of inequalities created and exacerbated by COVID-19 is truly shocking, High Commissioner tells Human Rights Council, www.ungeneva.org/en/news-media/meeting-summary/2021/09/lampleur-et-la-portee-des-inegalites-qui-ont-ete-creees-et

music, radio and TV services, and many other online applications have proliferated as a direct result of the pandemic.

This has added to the pressure and urgency of expanding the reach of mobile communications to under-served areas and of providing services such as online access to banks and financial services and payments systems all of which potentially benefit poorer and more marginalized communities.

For these reasons there is no need for the digital divide to widen again, but rather to speed up its closure. Digital should provide the channel for addressing this trend at a time when it is crucially needed for economic recovery and social stability. This raises an enormous opportunity for many developing economies to raise their productiveness by the simple measure of bringing greater access to women who are too often denied the opportunities to be fully involved in the economy or in many aspects of society.

For example, there is no reason for girls to be denied access to education when it is available online. What is needed are policies that ensure all the families involved have affordable means of access to smart phones or access to computers, either in their own homes and pockets or in local community centers or local schools. This is where economies can be proactive.

The results will be more women entering the workforce and adding to production and most likely to productivity. One strategic action governments could take where there are large pools of unemployed communities is to offer a basic income for them to assist as volunteers in the medical supply chain to move equipment and vaccines from ports of entry to warehouses to distribution points to hospitals and clinics, and to offer to those willing to take it up digital skills training associated with such supply value chains (SVCs).

This would not only produce immediate benefits to those involved and to the health of the community, but longer-term benefits in terms of a workforce with many basic digital skills. Thinking digitally means thinking strategically about how short-term solutions can result in longer term benefits and closing the digital divide in such ways could become the success story of the decade.

1.2.4 Green Digitalization and Sustainability

Digitalization is offering new ways to create environmentally sustainable ‘green’ growth. The examples are endless and growing by the day. They range, at the citizen and business-user end, from ways to monitor and reduce energy consumption in ‘smart buildings’, the replacement of oil and gas driven vehicles with electric or hydrogen-fueled vehicles controlled by digital operating systems, to carbon-reducing industrial processes that replace electrical-mechanical with digitally-controlled production process and SVCs where all processes from packing and trucking to customs and storage are digitally-managed, to the greatest challenge of all, the production of power by renewable sources of energy.

The term ‘green digitalization’ might be appropriate as a way to describe both the use of digital applied to provide green solutions such as energy-saving devices, and *digital by design*, as opposed

to *digital by default*, so that digital designs are made to be environmentally friendly, for example so their materials are easily recyclable.

As digitalization inevitably implies a greater demand for electricity, even as digital devices and processes become more energy-efficient, the challenge of green power supplies is basic to tackling climate change and the reduction of Green House Gases (GHGs). The Holy Grail, always apparently just out of reach, is nuclear fusion which is the process by which the Sun spreads its energy to Earth. Nuclear fusion has been successfully created but remains commercially difficult to scale up, and until that is achieved other measures are absolutely necessary to prevent global warming accelerating.

All other measures require digital technologies in their execution and power distribution, but they also require incentives for both public and private sectors to adopt them. Adopting climate change targets is insufficient unless the means of achieving them are also adopted. These may include carbon trading schemes, in which case the trading price becomes critical, or carbon taxes with and across borders which will need international agreements and collaboration such as the EU's proposed Carbon Border Adjustment Mechanism.[22] These policies also will need people trained in the skills of carbon auditing using the appropriate digital measuring instruments and these digital carbon auditing skills need to be shared with lower income economies.

Sustainability involves more than environmental protection, although that is the most pressing need. It also involves financial sustainability. The financial community is becoming increasingly aware of the danger of 'greenwashing' when approached to fund investments in environmental, social, and governance (ESG) projects and is developing standards by which to seriously judge their outcomes,[23] and mechanisms to reduce the risk-to-return ratio for private investors, especially in developing economies, through schemes of 'blended finance' which combine public and overseas development assistance funding (ODA) with private investments.[24]

A move beyond ESG is sustainable investing, otherwise known as socially responsible investing (SRI) or impact investing, which places a premium on positive social change by considering both financial returns and moral values in investments decisions.[25] There is an important link between ESG or SRI and the digitalization of banking and finance, as the latter is a means of providing far-reaching economic and social access to financial security.

---

[22] European Commission (2021) Carbon Border Adjustment Mechanism, https://ec.europa.eu/taxation_customs/green-taxation-0/carbon-border-adjustment-mechanism_en climatetrade.com/carbon-border-adjustment-mechanism/
[23] Network for Greening the Financial System (2021) Homepage, www.ngfs.net/en
[24] OECD (2021) Blended Finance, www.oecd.org/development/financing-sustainable-development/blended-finance-principles/
[25] S&P Global (2020) What is the difference between ESG investing and socially responsible investing?, www.spglobal.com/en/research-insights/articles/what-is-the-difference-between-esg-investing-and-socially-responsible-investing

1.2.5 Digitalization of Businesses Big and Small

As noted above, digitalization of businesses all along the SVC, from small farms through to manufacturers to end-user supermarkets is available to most enterprises, big or small. Digital technologies are driven by software algorithms processed through microprocessors in their electronics. A blended average fall in the price of such chips is estimated 2011-2021 at around 40% by the US Bureau of Labor Statistics. Over the previous twenty years, prices had fallen by over 60%.[26]

It is normal today to buy business equipment of all types fully digitized, and especially for small businesses the widespread digitalization of smart mobile networks offers enormous flexibility to transact business, including almost simultaneous payments where such systems have been introduced.

The ability of small businesses to reach new markets supports economic growth everywhere; as demonstrated by SMEs' contribution to GDP ranging from 40% to 60% in most APEC economies. SMEs also employ over half the workforce across APEC.[27] Further, individuals participate in globalization directly by using digital platforms to access information, to learn, find work, showcase their talent, and build social networks. These individuals gain social benefits from e-government services, are financially included, make purchases online, benefit from online education, or are assisted by remote medical facilities.

Digitization also usually involves a degree of miniaturization, and while in the initial marketing phase smaller more versatile and compact equipment is often premium priced, prices soon fall due to competition between vendors. This is why it is important for governments to support their micro, small and medium-sized enterprises (MSMEs) by not levying excessive import duties on digital equipment or restricting market entry.

While previously thought that digitalization of farming brought greater benefits to larger landholdings, it was discovered that small farms benefitted equally.[28] Linking farming, fishing and other rural area production to the SVCs that serve domestic city and overseas markets is a process that is enormously assisted by digitalization. At the rural end, aerial landscaping using drones to identify land use and the conditions of the soil, together with precision farming that uses digital technologies to increase yields and productivity, can be linked using blockchain technology and online administration and transactions to the manufacturing processors and end buyers. This is the basis of Industry 4.0 and can be applied to any economy whatever its overall state of development. It needs the full collaboration of state and private enterprise to secure the investments and create the legal and regulatory frameworks to make it happen.

---

[26] US Bureau of Labor Statistics (2021) Databases, Tables & Calculators by Subject, https://data.bls.gov/timeseries/PCU3344133344131

[27] APEC (2021) Small and Medium Enterprises, www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Small-and-Medium-Enterprises

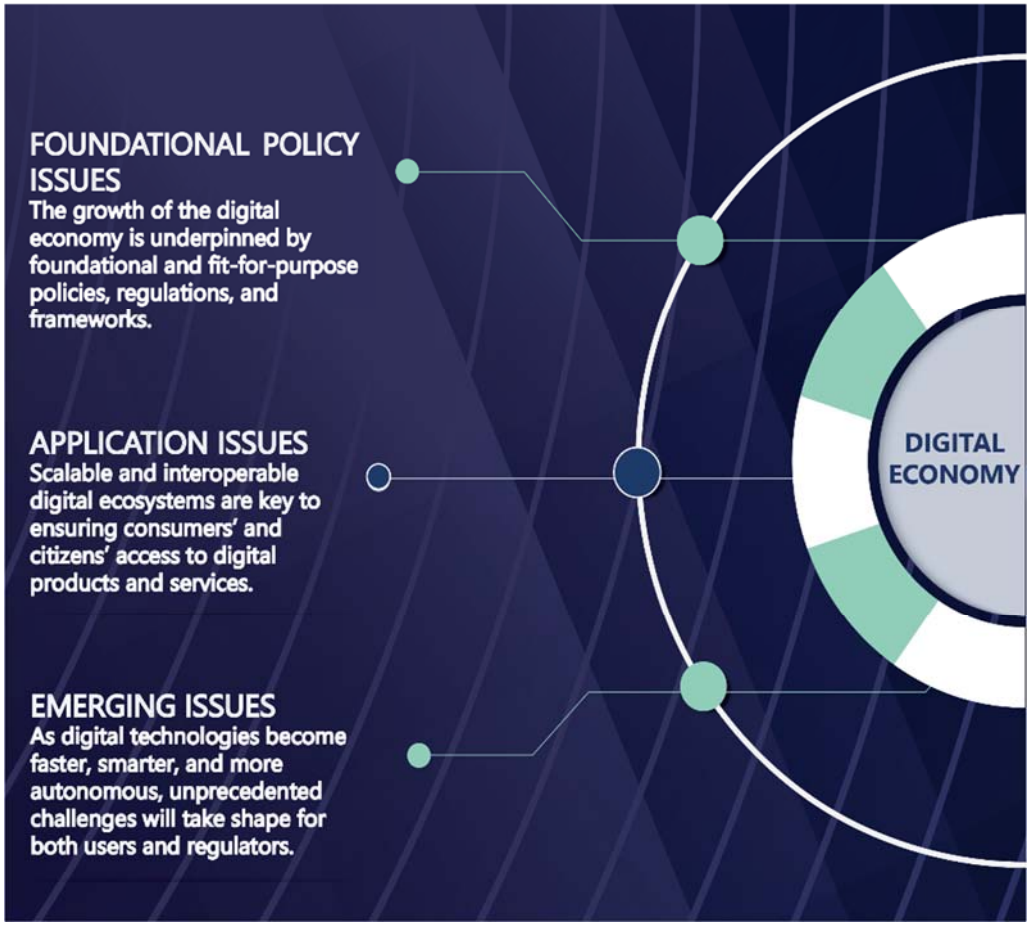
[28] World Bank (2020) Harvesting Prosperity: Technology and Productivity Growth in Agriculture, https://openknowledge.worldbank.org/bitstream/handle/10986/32350/9781464813931.pdf?sequence=6&isAllowed=y

2. Digital Economy Issues

The cross-cutting nature of the Internet makes it a fundamental input and driver for all other sectors, such as financial services, healthcare, education, tourism, and hospitality and, as illustrated, in recent years through the sharing economy, transportation, housing, and many more. It is because of this pervasiveness that holistically understanding the impact and enabling the benefits of the digital economy has become so important, and so challenging.

At the heart of this challenge are three main types of issues: **i) Foundational policy challenges; ii) Issues of application;** and **iii) Emerging disruptors.** These issues are examined separately within the Primer so as to clarify and examine each in its own context; where possible the interconnections and interlinkages are also identified; it is the interplay of each of these issues that makes grappling with the emerging landscape so challenging. Policy—and trade policy, in particular—is inherently about compromise; a key objective of this Digital Primer is to help raise awareness of the complexity of issues that need to be considered in setting digital policy agendas.

Figure 4: Digital Economy Issues



Source: Access Partnership (2021)

2.1 Foundational Policy Issues

2.1.1 Data Protection and Privacy

What is the issue?

Data protection and privacy are interconnected concepts (often used interchangeably) that concern the authorization of access to personal data. Data privacy refers to an individual's right to have some control over how their personal data is collected and used,[29] whereas data protection refers to an entity's responsibility to apply safeguards to the collection, storage, usage, and disclosure of personal data.[30] Data protection, including security, confidentiality and preserving the integrity of data, is central to data governance.

Why is it an issue?

Data is foundational to the burgeoning digital economy. As economies and businesses digitalize, there is an increasing dependence on personal data for the delivery of economic goods and services. Advances in technology also facilitate more sophisticated use cases for personal data.

Acquiring, processing, and transmitting this data can be integral to some business models, so keeping the data secure is paramount to building consumer trust. It is in the interests of all stakeholders that data privacy and protection measures are in place and are seen as thorough, transparent, and fair. Robust measures help to ensure that technological developments remain geared towards improving peoples' quality of life, as well as creating economic opportunities.

As such, domestic data protection and privacy frameworks should be expected to be able to support sustainable growth in the digital economy by establishing a high standard for data protection, and increasing users' trust in those who collect and use their data. However, data protection and privacy frameworks can differ quite significantly from jurisdiction to jurisdiction. Consequently, navigating and interpreting disparate compliance requirements is often a challenging and costly process, especially for MSMEs.

The alignment or harmonization of privacy requirements through the use of accepted international standards such as the OECD Privacy Guidelines or the International Organization for Standardization's (ISO) ISO/IEC 27701, and the adoption and use of data transfer mechanisms, can allow for the reconciliation of different domestic requirements. The use of such mechanisms can also facilitate the safe and seamless exchange of data across systems in different jurisdictions (i.e., interoperability), as well as their reusability across different systems, for different purposes (i.e., comparability).

---

[29] IAPP (2021) What does privacy mean?, https://iapp.org/about/what-is-privacy
[30] IAPP (2021) Glossary of Privacy Terms, https://iapp.org/resources/glossary

What are some considerations and challenges?

The needs for data privacy to be respected, protected, and secured, are important, but also need to be balanced with the needs of businesses and the economy overall to benefit from data transfers and data exchange. Going too far in either direction—either too open or too restrictive—can have profoundly negative impacts on either growth or trust.

Compounding this challenge is the need for privacy requirements across sectors to be respected and interoperable. Sectoral privacy requirements, such as in finance, health, education, and so on, can sometimes be seen to be different in implementation. In such cases, if not aligned from the very top of government, different sectoral requirements will not interact—a development we are seeing develop both between economies and within economies.

Data protection frameworks have two functions, foremost of which is to protect the data privacy of individual citizens. Importantly, the framework should also enable society and the economy to benefit from the data-based digital economy. Data-driven technologies have a growing role in providing useful and beneficial services to society. Whether in entertainment or education, finance or healthcare, innovation based on the use of data will continue to be a growing contributor to the economy and to society's wellbeing.

Given that data-driven business models and use cases are rapidly evolving, there is a need to have agility in data protection frameworks in order to avoid rapid and frequent amendments, and continue to balance innovation with protection and enhance trust (i.e., still hold data owners accountable for the personal data that they have access to and use).

A one-size-fits all consent (or authorization) rule does not work in an evolving technological environment and should be 'future-proofed'—by allowing flexibility in obtaining consent appropriate to the context in which it is being sought to be used. Consent provisions are often constructed based on either a paper-based environment or a web-based user interface. In those contexts, affirmative consent (in some cases, for each use of data) at the time the data was being provided by the data subject was the norm, and the expectation that all uses for the information being collected could be anticipated.

With the advent of new interfaces, such as mobile apps and devices, and devices without text input (e.g., voice-input systems like IoT home assistants, or devices which collect potentially personal non-text data such as through location trackers), and innovative data-driven interactions for users (systems that use the information about a user's behavior to produce a result for the user), existing frameworks requiring written or web-based advance express consent for the use of data may be cumbersome, and potentially present obstacles to innovation in features and services for users.

Advances in areas such as data analytics, artificial intelligence (AI), machine learning and the Internet of Things (IoT), will depend upon flexibility in the use of data while ensuring concomitant data protection. These uses of data portend the future of the digital economy and are already becoming significant contributors to the economy and employment with the potential for exponential growth.

However, insufficiently flexible consent-based models for privacy may constrain the proliferation of new technologies as they depend upon the collection of personal data in real-time and the transfer of collated and controlled data to neural networks and big data algorithms to process. For example, in the context of data analytics or machine learning, *even if* these technologies were able to procure consent before collecting data, the exponentially escalating combinations in which data can be interconnected nearly instantly will render it impossible to determine the original point of and purpose for consent.

Further, while many jurisdictions have recognized that implementing a data breach notification requirement can help mitigate the impact of a breach and ensure that adequate steps are taken to address the issue, there is no universal consensus around notification thresholds and timeframes. Some jurisdictions have established threshold definitions which are too ambiguous or easily triggered, resulting in problems of over-notification which creates unnecessary confusion and increased compliance costs. This can also risk leading to notification fatigue, whereby users who have shared data with organizations begin ignoring notifications because they receive such a large number that appear to have no relevance to them.

Requirements should thus be harm-based, with parameters set out in a way that conveys the expectation for organizations to act upon serious breaches, yet avoids imposing prescriptive definitions and thresholds that could result in over-notification and/or unnecessarily raise compliance costs.

Examples of emerging practices

Mechanisms that seek to facilitate interoperability across data protection and privacy regimes have emerged, allowing innovative digital offerings to penetrate domestic markets, and at the same time it is ensuring the safe and secure flow of data.

- The **Japan-EU Agreement**, for example, provides grounds for the mutual recognition of each other's data protection system as providing equivalent protection of personal data—allowing data to flow freely between the two economies.[31]
- The EU also issued an adequacy decision in December 2012 regarding New Zealand's **Privacy Act**.[32] New Zealand's Privacy Act was subsequently amended with guidelines for adequacy with other jurisdictions, in the form of Privacy Principle 12—though the comparability of safeguards defined in Principle 12 is assessed by disclosing agencies.[33]

[31] European Commission (2019) European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421
[32] Office of the Privacy Commissioner (2021), New Zealand-EU data protection adequacy reporting, www.privacy.org.nz/publications/reports-to-parliament-and-government/reports-on-new-zealand-adequacy-to-the-european-commission
[33] Parliamentary Counsel Office (2021), Privacy Act 2020, www.legislation.govt.nz/act/public/2020/0031/latest/LMS23376.html

Jurisdictions are modernizing their approaches on consent to reduce the burden on consumers, and ensure continued innovation.

- For example, in recognizing that "relying only on consent for the collection, use and disclosure of personal data may have deleterious effects",[34] Singapore in 2020 revised its **Personal Data Protection Act (PDPA)** to create grounds for data processing beyond explicit user consent by expanding the scope of "deemed consent" to include the secondary use personal data for business improvement purposes such as operational efficiency and service improvements; developing or enhancing products or services; and knowing the organizations' customers.[35]
- Australia, taking a different approach, is considering the use of layered notices or standardized icons and phrases to limit the informational burden on individuals and help them more effectively understand how their personal data is being used.[36]

There are also examples of robust data protection and privacy frameworks.

- The Philippines' Data Privacy Act requires data breaches to be reported when the data controller believes that there has been unauthorized access to sensitive personal information or other information that may be used to enable identity fraud which would result in serious harm to the affected data subject.[37] In this example, the threshold for the breach notification is established clearly and is not easily triggered by non-consequential breaches.

Key takeaways

- For a business, data protection addresses security, confidentiality, and preserving the integrity of data, including personal data. Regulators therefore need to create an environment that encourages participation and self-regulation to minimize risk and provide robust data protection.
- Provisions should incentivize the development and use of privacy enhancing technologies and methods—that is, data protection policies should encourage accountability to address risk of harm to individuals rather than establish a prescriptive set of compliance requirements.
- Requirements should be clear and fit-for-purpose and should be applied consistently and transparently across government and industry Data governance is most agile when it is technology neutral and based on accepted international standards and practices.

---

[34] Personal Data Protection Commission Singapore (2017) Public consultation for approaches to managing personal data in the digital economy, www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.pdf?la=en

[35] Personal Data Protection Commission Singapore (2021) Advisory guidelines on key concepts in the personal data protection act, www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en

[36] Australia Government Attorney-General's Department (2020) Privacy Act Review Issues Paper, www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf; Lexology (2021) What to expect from the impending release of the Privacy Act Review Discussion Paper, www.lexology.com/library/detail.aspx?g=3f36beb4-2204-45b3-a2ac-3a78e4a97667

[37] National Privacy Commission (2021) Data Privacy Act of 2012, www.privacy.gov.ph/data-privacy-act

- To avoid unnecessarily increasing compliance costs in international trade and friction in essential cross-border transfers of data, economies should actively look to the use of interoperability mechanisms that facilitate the standardization of compliance requirements.

2.1.2 Cybersecurity

What is the issue?

Cybersecurity relates to the protection of organizations, individuals and networks from digital attacks.[38] Digital attacks may involve the unauthorized access, modification and extraction of data, the theft of proprietary information, and the purposeful incapacitation of critical infrastructure, depending on the scale and intention of the attack in question.

Perpetrators of such attacks—also known as threat actors—may be profit-motivated and engage in ransomware attacks or data theft at various scales at the behest of private criminal syndicates or on an individual basis for financial gain. Jurisdictions may also facilitate cyber-attacks, with the aim of conducting espionage, data theft or infrastructure destruction, often using coordinated groups of threat actors—known as Advanced Persistent Threats (APTs). As digital applications and services become increasingly commonplace, threat surfaces through which threat actors can access information and conduct operations have increased exponentially.

Why is it an issue?

The risk of cyberattacks is increasing—rapidly—and will only continue to increase. Particularly, in an interconnected world. This is, and should be, of particular concern to the economic security of governments.

As data becomes the lifeblood of the economy, our understanding of what is critical infrastructure is also changing. A financial sector clearing house, a domestic health system, an interconnected payments system all begin to become crucial to the real-time functioning of the economy. What we used to call critical infrastructure has now changed, as is being recognized in a number of economies. With threats to the finance sector emanating from the communications and IT sector(s), threats to the health sector emanating from the payments sector, threats to the agriculture sector emanating from the customs sector, and so on, the need for government agencies to collaborate and set a common framework—drawing from international best practices—managed from the top of government, has become an imperative.

Cybersecurity has a significant impact on digital trust, and often intersects with discussions regarding the safeguarding of personal data— while also having growing implications for businesses' and governments' vital infrastructure. Governments and private sector entities across the region are making use of ever larger amounts of personal information in the design and implementation of digital applications such as digital identities and artificial intelligence (AI) algorithms. Attacks which can overcome the protections afforded to data stored and gathered for such purposes may result in

[38] Cisco (2021) What is Cybersecurity?, www.cisco.com/c/en_sg/products/security/what-is-cybersecurity.html

threat actors gaining access to sensitive personal information, leading to inconvenience or even identity theft, for data subjects.

This can in turn seriously compromise digital trust and impede digital engagement, as governments and private sector entities may appear incapable of protecting the data which has been placed in their care, or apathetic to the consequences of its loss. Should this happen, governments may find it more difficult to secure the public mandate to implement digital government initiatives more widely, while businesses may see uptake on digital products and services stagnate or fall, thus limiting the rate at which the digital economy can expand and the potential growth of digital trade.

Growth in the quantity of threat surfaces available for threat actors to act upon is a further challenge. The COVID-19 pandemic has accelerated the shift towards digitalization substantially and served as a boon to the digital economy. E-commerce is noted as being a major beneficiary, with significant proportions of offline retail activity shifting online since the start of the pandemic—resulting in the rise of e-commerce's share of global trade from 14% in 2019 to 17% in 2020.[39]

Governments have also taken the opportunity to implement increasingly holistic digital government initiatives, including those aimed specifically at addressing COVID-19 and other healthcare related issues, such as contact tracing. These developments potentially expose greater amounts of consumer and citizen data to cyber-attacks and increase the risk of cyber theft through e-commerce account hijacking, along with identity theft, and the loss of highly sensitive medical and biometric data.

The increasing linkage of critical infrastructure and supply chains to digital management systems and frameworks increases the potential impact of cyber-attacks on lives and livelihoods. Attacks perpetrated through unsecured threat surfaces have the potential to incapacitate telecommunications systems, transport infrastructure, medical equipment, and energy transmission networks, and cause widespread chaos—especially in heavily urbanized environments.

Historical attacks such as the catastrophic WannaCry and NotPetya ransomware attacks have demonstrated the capacity of cyberattacks to cripple vital government and business infrastructure in affected economies,[40] while the Stuxnet worm demonstrates how malicious software can be designed by state actors to target specific activities or functions.[41]

---

[39] UNCTAD (2021) COVID-19 and e-commerce: a global review, https://unctad.org/system/files/official-document/dtlstict2020d13_en_0.pdf

[40] Tech Crunch (2021) Two years after wannacry, a million computers remain at risk, https://techcrunch.com/2019/05/12/wannacry-two-years-on; DarkReading (2020) 3 years after notpetya, many organizations still in danger of similar attacks, www.darkreading.com/threat-intelligence/3-years-after-notpetya-many-organizations-still-in-danger-of-similar-attacks

[41] CSO Online (2017) What is Stuxnet, who created it and how does it work?, www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

What are some considerations and challenges?

A significant challenge, alongside the growth in threat surfaces, is the explosion in both quantity and sophistication of cyber-attack tools, alongside their growing accessibility and evolutionary mode of development. An illustrative development in this context was the leak in 2017 of the cyberattack exploit known as EternalBlue, which took advantage of a 'zero-day' vulnerability present on Microsoft systems to execute code on target systems.[42] 'Zero-day' vulnerabilities are understood as systemic vulnerabilities which are unknown or unaddressed by the operators of the systems which they compromise.

The EternalBlue zero-day was utilized by the Buckeye attack group in 2016 in attacks conducted in Europe and Asia, before being leaked online by the Shadow Brokers hacker group.[43] EternalBlue was subsequently used in both the WannaCry and NotPetya attacks and continues to be in circulation and use to the present day—representing the most-seen type of attempted exploit in 2020.[44] The persistence of EternalBlue even past its exposure and patching is a testament to the fragility of technical software maintenance practices globally, and represent the lasting, evolutionary threat a single effective cyber-attack vector can represent, even when considering active government and private sector mitigation efforts.

A consideration of note in this context is the need to balance government initiatives to facilitate law enforcement in the context of digital technologies with an over-arching agenda calling for the limiting of threat vectors. This challenge is embodied in ongoing discussions regarding the need for law enforcement backdoors into otherwise encrypted software.

Such measures would mandate the existence of tailor-made threat surfaces through which only law enforcement agencies would have access to encrypted information and software. However, this would principally be equivalent to requiring software manufacturers to engineer zero-day exploits for law enforcement use, which could perceivably be penetrated by unauthorized entities as well.

Examples of emerging practices

- The National Institute of Standards and Technology in the United States released the **NIST Cybersecurity Framework** in 2014. The NIST Cybersecurity Framework is a list of standards, guidelines and practices aimed at assisting governments and businesses of any scale to prevent, detect, respond to, and recover from cyber-attacks.[45] The NIST framework identifies five main functions that organizations must address, namely Identification, Protection,

[42] Center for Internet Security (2019) EternalBlue, www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf
[43] Symantec (2019) Buckeye: espionage outfit used equation group tools prior to shadow brokers leak, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit
[44] SentinelOne (2019) The NSA-developed exploit that just won't die, www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/; Bank Info Security (2021) Why does EternalBlue-targeting WannaCry remain at large?, www.bankinfosecurity.com/blogs/does-eternalblue-targeting-wannacry-remain-at-large-p-3002
[45] National Institute of Science and Technology (2021) Cybersecurity Framework, www.nist.gov/cyberframework/framework

Detection, Response and Recovery. High-level categories and accompanying subcategories address specific areas for controls to be considered under each of these five functions, and link to standards such as ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27017. The NIST Cybersecurity Framework is treated as a 'living document', with an updated version 1.1 being released in 2018.[46]

- The Cyber Security Agency (CSA) of Singapore has committed to the regular conducting of **Exercise Cyber Star**, a cross-agency, cross-sectoral cyber crisis management exercise intended to improve Singapore's crisis response capabilities and readiness in the case of a cyber-attack. The latest and largest exercise, conducted in 2019, involved more than 250 participants from both the private and public sectors. Representatives from 11 critical information infrastructure sectors participated, representing the government, infocomm, energy, aviation, maritime, land transport, healthcare, banking and finance, water, security and emergency, and media sectors.[47]

Key takeaways

- Cyber threat actors have grown in number and diversity and are becoming able to exploit a growing range of threat surfaces, which expand and emerge with the progressive adoption of digital applications and services across a wider audience.
- Cybersecurity has significant implications on digital trust, and therefore the ability of both governments and businesses to assure citizens and consumers of the utility of digital applications and services.
- Cybersecurity has further implications on critical infrastructure and supply chains, and insufficient attention paid to the issue can result in poor outcomes involving the loss of data and money, as well as the destruction of infrastructure and potentially the loss of life.
- There has been growth in the quantity, sophistication and persistent utility of cyberattack tools available to threat actors, especially in the context of ongoing processes of ongoing evolutionary development which build on existing tools to produce new outcomes.
- Growing awareness of the importance of cybersecurity has led to the development of new approaches to holistically address cybersecurity issues, including the creation of domestic standards or certifications for cybersecurity, and domestic or regional-level cross-agency collaborative exercises to maintain cybersecurity readiness.

[46] National Institute of Science and Technology (2021) Cybersecurity framework - evolution of the framework, www.nist.gov/cyberframework/evolution

[47] Cyber Security Agency of Singapore (2019) 11 CII sectors tested on more complex cyber attack scenarios, www.csa.gov.sg/news/press-releases/exercise-cyber-star-2019

2.1.3 Competition Policy

What is the issue?

Competition policy puts in place fair, open, and transparent rules to enable participation, productivity, and innovation in markets to benefit consumers, and businesses. Authorities seek to maintain market competition by prohibiting anti-competitive conduct, including anti-competitive agreements between competitors, abuse of a dominant position, and mergers that substantially lessen competition.

Competition policy also encourages government to develop pro-competitive policies and some competition authorities advise government agencies on a wide range of competition issues, including the impact of specific government initiatives on competition in the affected markets and the structure of public procurement.

To date, there has been a broad consensus that the goal of protecting and maximizing consumer welfare (i.e., the benefit to consumers when the price they pay for a good or service is lower than the maximum amount they would be willing to spend)[48] is and should be the cornerstone of competition policy.[49]

However, digital platforms have been increasingly associated with changing the rules of the game—through the dual- and multi-role that platforms play, horizontal and vertical integration concerns, network effects, 'free' services, use and control of data, and the 'winner takes all' approach. Not surprisingly this has raised concerns that digital platforms act as gatekeepers, with the power to create their own rules resulting in unfair conditions for business and consumers (e.g., higher prices, lower quality and less choice and innovation),[50] and given rise to a growing debate about whether competition laws and regulations from the pre-digital era remain fit for purpose and are able to curb market power in the digital economy.[51]

Why is it an issue?

In pre-digital economies, unregulated monopolies drive prices up, reduce consumer choice, reduce wages and stifle innovation. These are not inevitable outcomes. Well-governed monopolies can serve the social good, be innovative and bring the efficiencies of economies of scale (lower costs) and the benefits of economies of scope (wider choice).

---

[48] OECD (2005) Consumers' surplus, https://stats.oecd.org/glossary/detail.asp?ID=3176
[49] The University of Chicago Law School (2019) Reassessing the Chicago School of antitrust law, www.law.uchicago.edu/news/reassessing-chicago-school-antitrust-law
[50] European Commission (2020) Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN
[51] Lina Khan (2017) Amazon's Antitrust Paradox, www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyyeh.pdf

Traditional mainstream economic theories of perfect and imperfect competition were used to explain these outcomes, and the theory of contestable markets was used to explain that within a monopoly some sectors were in principle 'contestable', meaning if profit margins were above the competitive 'norm' then new entrants would threaten to drive them down and this threat alone *could be sufficient* to force the monopoly to act competitively.

If other sectors across the monopoly business were not contestable, then this either implied a 'natural monopoly' in which the optimum economies of scale (lowest marginal costs) outgrew the size of the market being served, or that the barriers to entry were too high—initial investment requirements (sunk costs) might be too great, or the task of winning customers away from the dominant company were stymied due to tie-in contracts or predatory (below cost) pricing, etc.—to permit effective competition. In both cases there was a case for regulatory intervention.

Some have argued that competition in the digital environment takes place on a different basis to the physical environment—noting that rather than competing on price and quality, digital competition is based primarily on innovation and the development of new technologies that will sweep away the old.[52] However, evidence now points to technology and innovation being used to entrench rather destroy market power, and that network effects, as well as upstream and downstream purchases, lead to further entrenchment.[53] Addressing this needs to be carefully considered to ensure that the benefits of the digital economy—particularly digital technologies and innovation—are not curtailed.

As with pre-digital monopolies, digital monopolies create similar barriers to entry: the economies of scale and scope that companies like Facebook, Apple, Amazon, Netflix, Google (the FAANGs) and others have achieved create almost insurmountable barriers to entry, and although start-ups can identify new applications, content or modes of communication, they easily fall prey to either being acquired by (e.g., killer acquisitions) or having their product replicated under a different guise by the monopolist. Indeed, the aim of being acquired can be the motive of the start-up and of the venture capital supporting it. Being acquired can be a faster and less risky route than aiming to create a market.

The key distinguishing feature of many of these digital players is the platform they create. The platform enables access to both sides of the market, bringing supply and demand together, often though not always, offering the platform owner monopsony power over suppliers and monopoly power over buyers.

Regulators face challenges here because the traditional metric to judge market power is the ability to manipulate prices. Many digital platform businesses typically charge nothing to consumers. For example, there is no charge for browsing the Web, using search functions, for chat and texting, for

[52] Centre for Competition Policy (2021) Competition and innovation in digital markets, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003985/uae-ccp-report__1_.pdf

[53] OECD (2019) Competition in the digital age, https://oecdecoscope.blog/2019/05/31/competition-in-the-digital-age

posting videos, and often downloading or streaming content. The 'price' paid by the consumer is to share personal information, including anything from demographic data (age, ethnicity, nationality), location and travel data, sexual orientation, contact lists, preferences in shopping, in music, political allegiance, state of health, and so on. This information is data to be monetized by the platform company, sold to commercial and even political organizations, used to charge advertisers who want targeted audiences, and used to position the products and services of the digital monopolist itself. *Data* is market power.

On the monopsonist side of the market, the platform company has extensive access to its suppliers' online customers and sales, has the power to discriminate between suppliers, and achieves asymmetric information. It knows more than either the suppliers or the customers, and can use algorithms to predict market trends, events and other strategic information. Digital platform businesses have more global market power than was ever possible in pre-digital economies.

Competition authorities are analyzing an increasing number of cases involving digital platforms,[54] and there are concerns that:[55]

- Some platforms exercise control over whole platform ecosystems in the digital economy and are structurally extremely difficult to challenge or contest by existing or new entrants, irrespective of how innovative and efficient they may be;
- Acquisitions and integration of secondary business lines create conflicts of interest and impact competition in upstream or downstream markets;
- Large online platforms engage in unfair conduct like self-preferencing practices, namely, actions by a platform which are designed to favor its own products or services over those of its competitors; and
- Lack of contestability hampers competition and innovation in digital markets. High barriers to entry or exit, including high investment costs and no or reduced access to key inputs such as data make the entry of new players difficult.

What are some considerations and challenges?

Digital business models offer enormous benefits in terms of choice of new and innovative services, availability or reach on a domestic and often international scale, and delivery over ever-faster broadband connections. Large digital platforms are cross-jurisdictional, and therefore the effort to promote competition in the digital environment will require effective cooperation *between* economies—even on a global scale.

[54] APEC (2019) Competition policy for regulating online platforms in the APEC region, www.apec.org/Publications/2019/08/Competition-Policy-for-Regulating-Online-Platforms-in-the-APEC-Region
[55] European Commission (2020) Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf

Digital players are altering what it means to be a buyer/seller, producer/consumer, employer/employee—effectively blurring, challenging, and even toppling traditional roles and responsibilities. Digital players, including those that own and operate online platforms, have been expanding their business to develop large ecosystems of complementary products and services around their core service.

There is a distinction to be made between a digital aggregator and a digital platform business, although in practice the lines between the two are blurred. An aggregator such as Facebook or YouTube aggregates the inputs, such as videos, posts, or songs of users and harvests their data. A platform business provides a platform for vendors or content creators to offer their services, but also often provides the payment mechanisms to realize the sales, and has access to their data such as sales volume and type. Aggregators also provide commercial platform services within the scope of their business. In both cases, the greater the scale and scope of their services, the more attractive they become to potential users and customers.

With digital aggregators and platforms alike, network effects often contribute to market dominance, since the value of a product increases when its consumption by others increases. For example, Google's search algorithm improves with a higher search volume and Facebook's social features work better the more friends share content, Uber's ride-sharing application is strongest when there are more than enough drivers to meet demand, and the more sales made through Lazada's platform the more vendors wish to use it. In theory, network effects are beneficial for consumers, as they provide a wide range of services that can be obtained on demand and at lower costs, with consumers benefiting from a one-stop-shop.

Digital platforms and services rely on all types of data to be able to function properly. Whether they take place on an e-commerce platform or a food delivery application, digital transactions data needs to be transferred between users, customers, web merchants, payment system operators, card companies, and many other intermediaries. Access to data is thus becoming an undeniable cornerstone of competitiveness. Access to large pools of data is a key topic in ongoing and forthcoming conversations, and other mechanisms which aim to redistribute market power away from data-rich incumbents.

Acquisitions by digital platforms have become common where incumbents use their substantial cash reserves to buy-out competitors or emerging companies that offer innovations that have the potential to become competitors. These are sometimes referred to as 'killer acquisitions', especially in cases where the innovation is abandoned as a means of preventing competition. While killer acquisitions are a way to ring-fence the success and ultimately market dominance of many digital companies, acquisitions of digital companies, especially of start-ups that have insufficient capital to scale up to become fully competitive without outside financing, are an important part of the digital ecosystem.

Further, the interplay between competition law and policy (e.g., defining markets, assessing dominance) and other forms of regulation that are being applied to digital markets and digital players (e.g., registration/local presence requirements, data protection and privacy, consumer

protection, etc.) makes close collaboration between different regulators of increasing importance. Prior to overhauling a specific set of rules or regulation, such as competition policy, government as a whole also needs to consider whether amendments to other frameworks (such as data protection or telecommunications) may be better placed to address concerns (e.g., data breach notification requirements could be strengthened to address consumer concerns, as well as ensuring adequate consent or notification for the use of data, rather than overhauling or placing these requirements within competition policy).

For example, careful management of data governance frameworks is key to ensuring that search and switch costs remain affordable. An overabundance of consumer data concentrated within a single dominant platform can disproportionately raise switch costs and thus inhibit fair competition. Users of platforms which use data to optimize service delivery may be disinclined towards switching to other services due to the inconvenience of having to provide information again or build user profiles from scratch. This can also be true of the more fundamental issue of access. A lack of data interoperability, and the absence of functional data transfer frameworks, can prevent consumers in some sectors such as finance and utilities from switching operators.

Further consideration also needs to be given to whether there is workable competition in the telecommunications sector—as this is a key precondition to competition in the digital economy. Without such competition, costs for innovators tend to be high and the ability to promote convergence across technologies is limited. But given telecommunications are a natural monopoly, promoting workable competition is difficult, particularly for smaller economies.

Examples of emerging practices

- **Europe**: The European Commission has proposed two legislative initiatives: the Digital Services Act (DSA) and the Digital Markets Act (DMA).[56] The DMA proposes an overhaul of competition rules for the tech sector, identifying and regulating potentially anticompetitive practices from 'gatekeepers', who have substantial power to control business' interactions with consumers in Europe.[57] It requires qualified online platforms to:[58]
    - allow third parties to inter-operate with the gatekeeper's own services in certain specific situations;
    - allow their business users to access the data that they generate in their use of the gatekeeper's platform;

[56] European Commission (2020) The Digital Markets Act: ensuring fair and open digital markets, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
[57] European Commission (2020) Digital Markets Act: Ensuring fair and open digital markets, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349
[58] European Commission (2020) The Digital Markets Act: ensuring fair and open digital markets, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

- provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper; and
- allow their business users to promote their offer and conclude contracts with their customers outside the gatekeeper's platform.

- **Australia:** Following a length inquiry in 2019, the Australian Consumer and Competition Commission (ACCC) made three explicit recommendations: i) the likelihood that a transaction could remove a potential competitor and the *amount and nature of data* that may be acquired in a transaction should be considered; ii) early scrutiny of acquisitions undertaken by large digital platforms should occur; and iii) restrictions on the default settings for installation of Internet browsers and search engines on computers, mobiles and tablet devices should be considered.

  The ACCC further found an imbalance of bargaining power between digital platforms and Australian news businesses.[59] To address this concern, the ACCC with direction from Parliament developed the News Media Bargaining Code (or News Media and Digital Platforms Mandatory Bargaining Code)[60] which is a law designed to have large technology platforms that operate in Australia pay local news publishers for the news content made available or linked on their platforms. The governments of the UK, Canada and India[61] are monitoring the launch of the News Media Bargaining Code which led to Facebook banning Australian news before coming to an agreement with the Australian government with amendments to the new law.[62]

  Australia also introduced a Consumer Data Right (CDR), which it has applied to the banking and energy sectors, with plans for application in the telecommunications sector as well. The CDR is a data portability initiative which grants consumers greater control over their data, requiring service providers within designated sectors to share information using a secure online system with other providers. Financial institutions have been required to share information with other financial institutions at the request of consumers, for example.

  This makes moving between products and services easier by reducing the costs required to search for information on alternative service providers, as well as the costs incurred by switching providers. The CDR is underwritten by Part IVD of the Competition and Consumer Act 2010 (Competition Act) and defined by the Australian Competition & Consumer Commission (ACCC)'s Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules).[63]

---

[59] ACCC (2019) Digital platforms inquiry, www.accc.gov.au/focus-areas/inquiries-finalised/digital-platforms-inquiry-0/final-report-executive-summary

[60] Parliament of Australia (2021) Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2021, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;page=0;query=BillId:r6652%20Recstruct:billhome; ACCC (2020) News media bargaining code, www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code

[61] BBC (2021) Facebook blocks Australian users from viewing or sharing news, www.bbc.com/news/world-australia-56099523;The Times (2021) Canada vows to follow Australia with new law after Facebook bans news, www.thetimes.co.uk/article/british-mps-round-on-bullyboy-facebook-after-it-blocks-news-in-australia-gv8d002rh

[62] BBC (2021) Facebook reverses ban on news pages in Australia, www.bbc.com/news/world-australia-56165015

[63] Government of Australia (2021) Competition and Consumer Act 2010, www.legislation.gov.au/Details/C2021C00248; ACCC (2020) Competition and Consumer (Consumer Data Right) Rules 2020, www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-rules-banking

- **Korea:** In light of the growing importance of online platforms the Korea Fair Trade Commission (KFTC) had concerns that the Monopoly Regulation and Fair Trade Law may be inadequate to tackle competition issues arising in the sector.[64] Hence KFTC plans to pursue a new sector-specific legislation "Act on Fair Intermediate Transactions on Online Platforms".

  The Act will be applied to platforms like delivery apps, app markets, accommodation apps, price comparison services and real estate. Under the Act online platforms must draw up a contract for a business using the platform. In addition, if an online platform abuses its market power it is subject to a penalty equivalent to up to twice the value pertaining to the violation.[65]

  While the National Assembly is still reviewing this Act, the revised Telecommunications Business Act was passed and takes effect on September 14, 2021, to regulate the mandatory use of in-app payment systems.[66] Korea is the first economy to introduce the law in the world. Under the revised Telecommunications Business Act, in effect, app store operators with dominant positions are not allowed to force app developers to use in-app payment systems owned or controlled by the operators as a condition of being distributed on the app stores or accessible on an operating system.
- **In the UK**, the government is planning to regulate online platforms and is establishing a new Digital Markets Unit, within the Competition and Markets Authority (CMA) aimed at encouraging competition within the digital sector. The new regulatory regime will regulate large technology firms classified as having 'strategic market status', meaning that authorities consider them to have substantial and entrenched market power.[67] The proposed UK regulation involves:[68]
  - A legally binding code of conduct for each company;
  - Pro-competitive interventions such as interoperability requirements that would enable consumers to have more control over their data;
  - Enhanced merger rules that would enable the CMA to investigate transactions between companies with strategic market status.

Key takeaways

- Increased use of digital technologies and innovation requires examination of who should be regulating various aspects of digital market participation, who should be ensuring accountability (and enforcement), and how those powers continue to work effectively in digital economy development.
- Increasingly, the intersection (and overlap in many cases) of regulatory responses—from competition policies to data governance requirements and emerging policy considerations—

[64] Kim & Chang (2020) Online platform regulation in Korea, www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=21945
[65] Business Korea (2020) Law to Be Enacted for Fair Online Platform Transactions, www.businesskorea.co.kr/news/articleView.html?idxno=52635
[66] CNBC (2021) South Korea passes bill limiting Apple and Google control over app store payments, www.cnbc.com/2021/08/31/south-korea-first-country-to-curb-google-apples-in-app-billing-policies.html
[67] PYMNTS (2020) UK moves to regulate big tech with proposed new watchdog group, www.pymnts.com/news/regulation/2020/uk-moves-to-regulate-big-tech-with-proposed-new-watchdog-group
[68] Verdict (2020) CMA gives UK government a template for regulating Big Tech, www.verdict.co.uk/cma-big-tech

are being examined and called into question. Navigating this intersection—and integration—between competition policies and broader digital regulation will be crucial in ensuring effective and fit-for-purpose policy making for digital markets.

- Competition authorities have also become sensitive to the growing importance of data. Large amounts of data in and of itself may not be problematic, but there is an increasing need for data to be factored into assessments as the ability to generate and collect data can create a competitive advantage, but an inability to access data can be a market barrier.
- The rise of digital platforms has led to a rethink of what regulations are needed to effectively address tech companies with market dominance. Responses can be expected to change as understanding evolves on how digital platforms have (or have not) upended traditional interpretations of competition.
- In the digital economy, business practices and models evolve very quickly—often much faster than regulatory processes. Investigations can take a long time, with remedies often coming after the fact. Although decision making should not be rushed, there is a need to increase the pace in which cases are processed.
- In order to make effective assessments, competition agencies need to cooperate and coordinate: i) at the domestic level between relevant agencies (e.g., ICT, finance, trade, and privacy); ii) between economies, particularly to address capacity building and resource constraints for developing economies; and iii) between economies to ensure cross-border knowledge sharing and/or joint investigations where digital players are present in multiple jurisdictions.

2.1.4 Online Consumer Protection

What is the issue?

Consumers expect the same level of protection when transacting online as if they were engaging in conventional 'brick-and-mortar' retail. To ensure this, online consumer protection involves deploying measures to protect consumers from fraudulent, misleading, or deceptive conduct when they engage in electronic transactions.

Such transactions may involve local retailers and vendors or those from further afield. As a consequence, many businesses and consumers transact in a range of jurisdictions with various e-commerce regulations. This has implications for advertising, cross-border regulatory and policing cooperation, product recalls, and digital platform markets, the latter of which often blurs the distinction between consumers and businesses.[69]

Despite enjoying greater choice in products and services through the Internet, consumers could be vulnerable to: i) misleading information provided by businesses, including confusion about the status and location of an online vendor; ii) unfair commercial practices; iii) unfair contract terms and conditions; iv) poor online payment security; and/or v) no mechanism for redress, especially for cross-border online transactions. While some jurisdictions have a legislative framework for online consumer protection, others are not equipped to act against online rogue traders at the domestic or global levels.

Why is it an issue?

The tools and techniques employed by digital platforms, including the collection, use, and presentation of personal data (and the use of AI algorithms),[70] have resulted in individualized and more convenient access to digital products, services, and content. On the other hand, it has also raised consumer protection concerns, most prominently the risk of profiling and the rise of discriminatory practices that may negatively affect consumers.

Digital platforms may lack transparency—thus preventing consumers from evaluating the value of the service they receive, as well as the underlying contractual relationship that is taking place.

Business models founded upon the free provision of products are not new: media companies have long made radio, television, or newspaper content available for free, funding their product through advertising revenues and classifieds. In the digital economy, new zero-price markets have emerged

[69] OECD (2021) Going digital: digital consumers, www.oecd.org/going-digital/topics/digital-consumers
[70] Federal Trade Commission (2020) FTC issues orders to nine social media and video streaming services seeking data about how they collect, use, and present information, www.ftc.gov/news-events/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services

with their own unique characteristics and large scope. Many consumers use at least one free digital product or service throughout a typical day.

From mobile gaming applications to social networks, plenty of technology companies offer some form of zero-price product or service, often designed to build customer loyalty, acquire user data, gain free publicity, or even to destabilize competitors. Regulators must consider the nature of the transaction between the user and the free product/service provider. If the characteristics of the transaction are challenging to define, then the relationship between service provider and consumer will also be hard to identify, rendering it difficult to apply the most appropriate regulatory measure or framework.

Many consumers are not also aware or are uncertain of their rights and responsibilities in consumer-to-consumer transactions, or about who to turn to when something goes wrong. Greater transparency is also necessary with regards to pricing practices, since search results on some platforms do not give the total price until it is difficult for a buyer to rescind an offer or a payment. On a similar note, some jurisdictions have established online dispute mechanisms, which help by offering a platform on which consumer issues can be resolved on a case-by-case basis through discussion between consumer and merchant. These can offer a pathway to adjudication by an independent dispute resolution body, if a case is not resolved to the satisfaction of all parties.[71]

Terms of use and privacy policies are often long and complicated, written in obscure legal jargon that is challenging for consumers to understand. Rather than explaining to users what the conditions are, these texts are drafted with the purpose of being a liability waiver for the company, to which consumers often uncritically agree in order to use the service. The shift towards mobile devices and the Internet of Things (IoT) only aggravates these concerns around terms and conditions, as it will become even more difficult for consumers to understand the extent and the ramifications of what they are agreeing to.

What are some considerations and challenges?

There is a growing focus on how digital platforms collect, use, and present personal information, advertising, and user engagement practices—and how this affects and/or is targeted at children.[72] The ubiquity of digital platforms in consumers' daily lives, combined with the rising sensitivity of the data they collect (social interactions, buying habits, personal preferences and interests, locations, personal schedules, and plans, etc.) makes user data an extremely valuable asset. Users are constantly tracked, monitored, and profiled, many times without their knowledge or consent.

[71] European Commission (2021) Online Dispute Resolution, ec.europa.eu/consumers/odr/main/?event=main.home2.show
[72] Federal Trade Commission (2020) FTC issues orders to nine social media and video streaming services seeking data about how they collect, use, and present information, www.ftc.gov/news-events/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services

AI algorithms enable advertising campaigns to be targeted with more specific understanding of an individual's customer's needs without substantial research cost, making marketing smarter and more effective. Another major business advantage is customer satisfaction since anticipating a customer's needs plays an increasingly important role in long-term retention. Indeed, an exceptionally designed recommendation engine can be the underpinning of an entire business model.

However, algorithms remain a mystery for consumers, in many cases by design.[14] Rarely do digital platforms offer any information on the way recommendations are selected, ranked, or displayed on content platforms, search engines, comparison sites, or online booking platforms. This has led to the emergence of consumer protection concerns stemming from the use of AI, most prominently the potential for profiling and the rise of discriminatory practices, such as price discrimination, that may negatively affect consumers.

Examples of emerging practices

- **Multilateral organizations**: UNCTAD and OECD have both set out principles regarding access to information on digital products, clear statements on terms of use, recommendations for consumer protection against deceptive practices, principles for privacy and data security protection, and measures to provide effective remedies and redress.[73] Through their reports, these organizations have offered robust principles around which effective frameworks may be set out.
- **Digital Trade Agreements:** In recognition of rising online cross-border transactions, a number of trade agreements have included provisions for online consumer protection, including:
    - Article 15 of Singapore-Australia Digital Economy Agreement, which encourages the maintenance of measures to protect consumers from "misleading and deceptive commercial activities"; [74]
    - Article 6.3 of the Digital Economy Partnership Agreement states "Each Party shall adopt or maintain laws or regulations to proscribe fraudulent, misleading or deceptive conduct that causes harm, or is likely to cause harm, to consumers engaged in online commercial activities. Such laws or regulations may include general contract or negligence law and may be civil or criminal in nature";[75]

[73] APEC (2020) Promoting consumer protection in digital trade: challenges and opportunities, www.apec.org/Publications/2020/06/Promoting-Consumer-Protection-in-Digital-Trade; UNCTAD (2016) United Nations Guidelines for consumer protection, https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf; OECD (2011) OECD Guidelines for Multinational Enterprises, www.oecd.org/daf/inv/mne/48004323.pdf

[74] MTI (2020) Singapore-Australia Digital Economy Agreement, www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Singapore-Australia-Digital-Economy-Agreement/Singapore-Australia-Digital-Economy-Agreement.pdf

[75] MTI (2020) Digital economy partnership agreement, www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Digital-Economy-Partnership-Agreement/Text-of-the-DEPA.pdf

  - Article 19.7 of the United States-Mexico-Canada Agreement (USMCA), which advocates implementing measures that "protect consumers from fraudulent or deceptive commercial activities";[76] and
  - Article 14.7 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) requires signatories to "maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities".[77]
- **Europe:** The EU's Unfair Commercial Practices Directive[78] was updated in 2018 to reflect digital developments that affect consumers.[79] The new rules allow for better enforcement and consumer protection rules around transparency of online marketplaces, transparency of online reviews, as well as penalties for cross-border infringements within the EU.
- **Korea:** The Act on the Consumer Protection in Electronic Commerce protects consumer rights and seeks to enhance market confidence by regulating matters relating to fair trade in goods and services by means of electronic commerce transaction.[80] The act prevents online businesses from using information without obtaining consent from the relevant person. online intermediary must explicitly inform consumers that they are not a party to the main supply contract.
- **Brazil**: The Consumer Protection Code, E-commerce Act and Internet Act, requires companies indicate information on the products and services available for sale, information concerning the service provider, terms of online purchasing, payment condition and product warranties.[81] In addition, purchasers have the right to withdraw and to be informed of their rights to cancel any contract and return purchased goods within seven days of conclusion of purchase or receipt of the product, for transactions that are concluded online or outside the provider's bricks-and-mortar location.
- **United States:** The Federal Trade Commission (FTC) is charged with protecting consumers in the marketplace. The FTC relies on 4 key tools: i) information sharing; ii) investigative assistance; iii) cross-border jurisdictional authority; and iv) enforcement relationships. The US SAFE WEB Act enables these international consumer protection tools.[82]

---

[76] Office of the United States Trade Representative (2020) Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

[77] DFAT (2015) TPP Text and Associated Documents, www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents

[78] European Commission (2020) Unfair commercial practices directive, https://ec.europa.eu/info/law/law-topic/consumers/unfair-commercial-practices-law/unfair-commercial-practices-directive_en#:~:text=Objective%20of%20the%20directive,-The%20objective%20of&text=EU%20rules%20on%20unfair%20commercial,techniques%20to%20influence%20their%20choices

[79] European Commission (2019) The New Deal for consumers: what benefits will I get as a consumer?, https://ec.europa.eu/info/sites/info/files/factsheet_new_deal_consumer_benefits_2019.pdf

[80] Fair Trade Commission (2021) E-Commerce, www.ftc.go.kr/eng/contents.do?key=508

[81] DLA Piper (2018) E-commerce in Brazil: practical specificities for complying with the Brazilian online market, www.dlapiper.com/en/us/insights/publications/2018/11/law-a-la-mode-27th-edition-november-2018/5e-commerce-in-brazil

[82] Federal Trade Commission (2016) International Consumer Protection, www.ftc.gov/policy/international/international-consumer-protection

Key takeaways

- Economies that enter into digital economy trade agreements, should include provisions for online consumer protection to create greater alignment and protection for cross-border transactions.
- Economies developing ecommerce laws can consider introducing online consumer protection if there is no policy currently in place.
- Economies that already have consumer protection laws in place, should review and update, where necessary in light of digital developments and ensure they have suitable enforcement tools to take actions against rogue online traders.
- It is important for all economies to educate consumers so that they can become informed, and this can be achieved by develop more consumer outreach materials and guidelines to raises the awareness of the risks with online transactions.
- International cooperation is required to support, enable, and safeguard cross-border transactions.[83] This may be fostered through digital economy agreements.

[83] APEC (2020) Promoting consumer protection in digital trade: challenges and opportunities, www.apec.org/Publications/2020/06/Promoting-Consumer-Protection-in-Digital-Trade

2.1.5 Intellectual Property (IP)

What is the issue?

The World Intellectual Property Organization (WIPO) lists intellectual property (IP) as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce."[84] Intellectual Property Rights (IPRs) refer to rights granted in law to persons or businesses over those creations of the mind, and cover areas such as: [85]

- Copyright (right that creators have over their literary and artistic works)
- Patents (exclusive right for an invention)
- Trademarks (sign to distinguish goods or services)
- Industrial designs (aesthetic aspect of an article)
- Geographical indications (goods with specific geographical origin and qualities)
- Trade secrets (confidential information which may be sold or licensed).

IPRs might belong to the original creator(s) or their employers, or their publishers, or whoever bought them as an asset. What is considered to be IP is changing in the digital environment, for example, digital technologies:

- have the potential to promote innovation;
- be used as a means of distributing content that is IP; and
- also be considered IP itself.

Whilst there is broad agreement on the importance of IPRs and their enforcement in the digital environment, the nature of the digital economy poses a number of questions as to whether IP systems continue to be fit for purpose.

Why is it an issue?

The principle behind IPRs is ownership as a reward for their inventiveness and to encourage further inventive efforts. This reward is in exchange for the benefits to society of access to technology and innovation. While IP plays an important role in incentivizing innovative technologies, it should also encourage the availability and access to technology and technology assets. Excessive protection of IP could frustrate the full benefits of digital trade, just as adequate IP protection could undermine incentives for innovation and creativity.

The digital economy has greatly improved the ability of creators, authors, businesses, and ISPs to disseminate goods, services, and content. This in turn has increased the incentives to innovate—but has also highlighted that IP settings now may be too strong in some areas, and too weak in others to promote necessary innovation. For example, copyright owners seek long term protection and more

[84] WIPO (2021) What is Intellectual Property?, www.wipo.int/about-ip/en/
[85] WIPO (2021) What is Intellectual Property?, www.wipo.int/about-ip/en/

substantive rights, whereas users seek less protection and further exceptions—fueling innovative uses. Flexible provisions will be required in order to effectively address entrenched and polarized views on these positions, and ensure protections are adequate and appropriate for the digital age.

The provision of content in the digital economy—including IP-protected content and data that may or may not be protected by IP—takes place on a quite different basis than in the physical economy. Digital delivery services are a means of distributing IP content, but services and IP are often treated as separate disciplines. This nexus between digital delivery services and IP is detailed and important, and this relationship needs to be better understood. Further, the 'bundling' of and provision of 'free' or subscription-based content provided by digital players needs to be taken into account in IP regimes, ensuring that IP rules do not become an inhibitor to innovation and consumer welfare in this area.

As digital transformation becomes the salient feature of economic development, new forms of inventiveness arise. Many of these are associated with the rise of e-commerce and digital platforms and the use of algorithms, and with the evolution of automated industrial and work processes. There is evidence that IP rules can act as an inhibitor to such innovation taking place. This has resulted in new business processes being subject to a range of IP protections, including copyright, patents and sometimes trade secrets. Software patents are a particular case in point where patent trolls and patent thickets have a deadening effect on innovation.

Without the right mechanism to regulate IP, international trade will be skewed as firms with patents (particularly in the United States) prefer to export more often to economies with better IPR policies. Developing economies tend to be more reliant on imports for the latest technologies to propel their economy, yet will be disadvantaged as often lack strong IPR policies. Under-representation in areas of IP use also means that we are not maximizing full potential to solve pressing challenges. This makes for unequal economic outcomes overall.

Unsurprisingly, sectors that are more vulnerable to imitation or copying are pushing to adopt stricter global IPR protection. Examples include pharmaceuticals, specialty chemicals, entertainment, publications and information technologies.[86]

What are some considerations and challenges?

Enforcement of IPRs is a particular challenge in the digital environment where methods of circumvention are readily available to consumers. Through the rise of social media, fake and counterfeit goods are causing loss of revenue and of reputation to branded items everywhere, and IP is easily stolen through hacking of company resources. Invoking the law maybe too little, too late, and therefore ineffective. This has promoted the legal protection of digital locks (of various kinds) allied technological protection measures.

[86] John Revesz (1999) Trade-related aspects of intellectual property rights, www.pc.gov.au/research/supporting/intellectual-property/trips.pdf

In the post-War period the US has been dominant in industrial invention, especially in IPRs in digital goods and services. The US first introduced IPRs into trade negotiations in the negotiations for what eventually became the 1994 North American Free Trade Agreement (NATFA) between Canada, Mexico and the USA, and the WTO 1995 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).

There is evidence that FTAs have played a strong role in promoting IP rights that are significantly stronger than those agreed under TRIPS. FTAs tend to be negotiated on a mercantilist basis with the interest of IP owners to the fore while there is much less input from consumers and future innovators. They are also negotiated separately from digital service commitments and the relationship between them overlooked. When engaging in trade negotiations, developing and smaller economies often feel they need exemptions or waivers from royalty payments, especially if they are to develop their digital and bio-technology sectors.

Available to poorer economies and businesses, especially small and medium-sized enterprises who cannot easily afford to pay royalties there are royalty-free digital software products that are made available under a GNU[87] General Public License[88] or GNU-GPL. These licenses offer the source-code free-of-charge and are motivated by the desire to see the widespread adoption and use of the software in question, such as the Linux operating system.

This is one criticism of how intellectual property rights (IPRs) are handled, that most IP resides or is owned by companies or financial groups in the richer economies, notwithstanding the fact that China now registers the most new patents each year, and this disadvantages poorer economies. The IP of pharmaceutical companies has particularly become an issue of debate during the pandemic.

IP enforcement can often lead to geo-blocking where restrictions are imposed on use or access in particular regions of the world which in turn prevents the operations of open markets and competition, and often complained about are IP 'trolls' who are persons who buy up IPRs for the sole purpose of squeezing more payments out of users.

The pace at which new patents are being created has accelerated in the digital age. For example, in the US, in 2020 almost 400,000 patents were issued compared with under 200,000 in 2000.[89] In terms of new patent applications, in 2016 China received 1.3 million, followed by over 600,000 in the US, over 300,000 in Japan, over 200,000 in the Republic of Korea and 160,000 in the EU.[90] These are staggering numbers, and it means that only global registration of an IP can assure protection, something beyond the resources of creators of IP in most developing economies. Certainly, no system is perfect, and even the quality of the patents is sometimes questioned, not least because the system for registering new patents and copyright are often overwhelmed with applications each of which should be thoroughly and carefully checked.

---

[87] GNU (2017) Overview of the GNU system, www.gnu.org/gnu/gnu-history.en.html
[88] GNU (2021) Licenses, www.gnu.org/licenses/licenses.en.html
[89] Statistica (2021) Number of patents issued in the United States from FY 2000 to FY 2020, www.statista.com/statistics/256571/number-of-patent-grants-in-the-us
[90] WIPO (2017) Patents, www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2017-chapter2.pdf

As IPRs currently apply to human created work and invention, there is debate about how this can be extended or modified to suit machine created work and invention. Concerns focus on whether AI is considered a creator and thereby, whether IP protection would apply to the machine created work and invention; protection over the algorithms and software; as well as the privacy rights in the large quantity of training data inputs.[91]

Examples of emerging practices

- **Singapore:** The Singapore IP Strategy 2030 (SIPS 2030) aims to strengthen Singapore's position of global hub for intangible assets and IP, build innovative capabilities, move up value chain and capture new growth opportunities.[92]
- **Europe**: In 2016, the EU Commission conducted an evaluation of the Directive on the Enforcement of IPR (IPRED) to further improve the application and enforcement of IPRs. IPRED has led to the creation of a common legal framework where the same set of tools is applied across the EU.[93]
- **ASEAN**: The ASEAN Working Group on Intellectual Property Cooperation (AWGIPC) has taken initiatives that include improving the speed and quality in patent prosecution in ASEAN.[94] For example, starting from June 2021, applicants can use written opinion(s) established by participating AMS IP Office(s) to accelerate the patenting process in another participating AMS IP Office.
- **Australia:** In May 2021, Australia announced that it will introduce a patent box for eligible corporate income associated with new patents in the medical and biotechnology sectors. The patent box will apply to companies for income years commencing on or after 1 July 2022.[95]

Key takeaways

- Digital technologies have changed the way we view what is considered IP—which includes digital technologies having the potential to promote innovation, be used as a means of distributing content (that is IP), and that means also being considered IP.
- The level of IP protection needs to be fit-for-purpose, in order to strike a balance between layering on IP protection (to spur innovation efforts) and not swinging to the other extreme of being too guarded, thus impeding innovation efforts.
- Enforcement measures (particularly technological protection measures) need to be balanced with corresponding downsides to innovation and consumer rights. Economies need to consider whether there are more effective enforcement strategies available that will promote consumer compliance on the basis that consumers endorse the belief that IP systems are in their own interests.

---

[91] WIPO (2020) Frequently Asked Questions: AI and IP policy, www.wipo.int/about-ip/en/artificial_intelligence/faq.html
[92] IPOS (2021) strategy to boost Singapore's position as a global intangible assets & IP hub unveiled, www.ipos.gov.sg/docs/default-source/default-document-library/singapore-ip-strategy-2030-media-release.pdf
[93] European Commission (2021) Enforcement of intellectual property rights, https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement_en
[94] ASEAN (2021) More Report Choices for the ASPEC Programme, www.aseanip.org/News-Events/Latest-News-Events/ctl/Details/mid/1956/aid/83
[95] Australian Treasury (2021) Patent Box consultation, https://treasury.gov.au/consultation/c2021-177849

- Economies need to consider what options are available to ensure that FTAs drive optimal IPRs and enforcement, rather than promote a 'maximalist' position. In ensuring an enabling regional environment, APEC has a key role to play.

2.2 Application Issues

2.2.1 Digital Identity

What is the issue?

Governments use identity systems to provide citizens with an official proof of identity, which can be used when interacting with government agencies, hospitals, or education and financial institutions, or employers. This often involves the collection and validation of personal information (such as name, address, date of birth), which are then demonstrated through credentials such as identity cards or unique identification numbers. [96]

A digital identity is "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions".[97] A digital identity can uniquely identify a person, and can be distinguished from an online identity, which is not unique. A digital identity can refer to a person, a legal entity such as an enterprise, or to a thing (such as a financial asset) or some connected objects such as IoT.[98]

Economies are increasingly deploying digital identification systems—which utilize digital technology from the initial capture of personal data to its validation[99]—which provide a single source of truth for a complete and standardized view of individuals' identities.[100] Digital identities enable verification and authentication of individuals for a wide range of in-person, online, and remote transactions, with less friction.[101]

Why is it an issue?

Everyday activities hinge on people being able to prove their identities—from enrolling in school, accessing basic social services, claiming pensions and social welfare payments, opening a bank account, obtaining a mobile phone, accessing healthcare, voting in elections, registering a business, or even crossing borders.[102]

Digital identity systems have the potential to transform the way economies and businesses' function by making it easier for all individuals to access services in a faster and convenient manner. When

[96] World Bank (2019) ID4D Practitioner's Guide, https://id4d.worldbank.org/guide
[97] GSMA, World Bank Group, and Secure Identity Alliance (2016) Digital identity: towards shared principles for public and private sector cooperation, www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf
[98] Technopedia (2020) Digital Identity, www.techopedia.com/definition/23915/digital-identity
[99] World Bank (2019) ID4D Practitioner's Guide, https://id4d.worldbank.org/guide
[100] ITU (2018) Digital Identity for Development Initiative, www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx
[101] World Bank (2019) ID4D Practitioner's Guide, https://id4d.worldbank.org/guide
[102] World Bank (2019) Inclusive and trusted digital id can unlock opportunities for the world's most vulnerable, www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

they are thoroughly authenticated, unique, established with consent, protect user privacy and offer users control over personal data, digital identities allow for streamlined systems and services that make identification easier and more robust.

This has been crucial aspect of accessibility and inclusion as digital transformation efforts ramp up, with COVID-19 amplifying and pointing to the pervasive role that digital enablement is going to play in each economy's exit strategies as economies begin to be opened up and re-inflated. From turning to digital channels to provide contactless and online remote procedures to process payments, including remittances and government disbursements; contact-tracing and QR code check-in requirements; for those in urgent need of medical attention, or seeking access to medical advice, make remote appointments or call for assistance; and to rolling out vaccination plans and looking towards vaccine passport recognition—these government services required individuals to digitally prove their identities.

For trade to take place, verifiable identifiers are important in all parts of the digital trade process across multiple parties where buyers, sellers, and service providers can prove and verify who they are and manage custody of goods. The ability to audit and authenticate to ensure that transactions are valid and made among the correct parties is also essential to combat fraud and money laundering.

Digital identification systems enable innovation in the public and private sectors, as well as enhancing compliance. They facilitate more responsive public and private services. Additionally, they reduce operational costs, cut response times, enhance security, and offer a platform for improved customer experiences and greater cross-agency collaboration.[103] Streamlined systems that make use of universal digital identification have the potential to save governments 110 billion hours of work, and by extension, reduce costs to the government.[104] The authentication systems involved in digital identification mean that government-to-person transfers become more transparent, and fraud is reduced as a result. Impersonation is far more difficult through this system, and payments for public salaries and social welfare programs, are rendered more secure.

Digitalizing identification systems allows for easier expansion of the coverage of government services, ensuring more people can participate more fully in social, economic, and political life. With digital identification systems in place, people can more easily make payments, register businesses, or create bank accounts. As a result, previously informal financial interactions are formalized, promoting financial inclusion. This is to the benefit of individuals, communities, and the economy more widely. Implementation of digital identification systems is estimated to create economic value equivalent to between 3 and 13% of GDP by 2030.[105]

---

[103] World Bank (2019) Inclusive and trusted digital id can unlock opportunities for the world's most vulnerable, www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

[104] McKinsey Global Institute (2019) Digital Identification: A Key to inclusive growth, www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#

[105] *Ibid.*

What are some considerations and challenges?

In terms of digital identity management, key areas of concern are security and privacy, particularly for biometric data. If a digital identification system is not sufficiently robust, it can jeopardize the personal data of citizens and residents. Databases containing a large volume of personal data (particularly unique biometric data) must be supported by an effective information security framework, as well as a well-designed digital identification system. The authentication process, too, must be designed with security as a paramount concern.

It is important to acknowledge concerns about how public and private sector organizations use personal data for the provision of online services. Metadata from these databases could potentially be used for profiling and surveillance.[106] This risk is amplified by the coexistence of facial recognition technology and biometric data.[107] Clear and effective privacy and data protection measures can raise the confidence of people to embrace the technology behind the digital identity system. This will be boosted further as the digital identity system facilitates the smooth delivery of government services. With adequate safeguards in place, and clear procedures that specify the treatment of the different sets of data and under specific conditions, trust in government systems will be enhanced.

There must also be consideration of the resources required to implement and maintain the digital identification system. With high levels of accuracy, integrity, and security of system assets and processes, efficiencies can be assured for a longer period of time. If systems are less secure, or use less up-to-date technology, they risk compromising the benefits of digitalization. Costs may rise and issues such as identity theft, normally quashed through the introduction digital identity systems, may proliferate.

Of paramount importance is the provision of unique identity profiles for individual users. This should be a cornerstone of any such system's development. With uniqueness built into the system, instances of mistaken identity or identity theft can be isolated or eliminated.

An associated issue, which will emerge with greater importance in the future, is the interoperability of the system with other identity systems. Economies will likely adopt different systems, but there are rewards to be reaped if the systems are interoperable and the data portable. If the system can be used in parallel across economies, and in association with institutions such as banks, insurers, multinational service providers (for mobile phone coverage for example), convenience for users will be maximized, and costs minimized for all parties involved.

---

[106] Access Now (2018) National Digital Identity programmes: what's next?, www.accessnow.org/national-digital-identity-programmes-whats-next/; ITU (2016) Digital Identity Roadmap Guide, www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf

[107] Wired (2018) Digital IDs are more dangerous than you think, www.wired.com/story/digital-ids-are-more-dangerous-than-you-think

Digital identification systems can allow easier access to all services requiring proof of identity, and can foster inclusion. However, systems must also be paired with strong digital infrastructure, since the reach of a digital identification system is only as far as the infrastructure it uses, and it should also be appropriate to the context of the economy adopting it; geographical and cultural dynamics must be accounted for when designing and implementing the identification system. The systems must also be sensitive to groups unable to share biometric identifiers, such as older people, people with disabilities or those who do intensive manual labor, who may not be able to share fingerprints.[108]

Examples of emerging practices

- **Singapore:** SingPass (Singapore Personal Access) is the gateway to e-government services in Singapore and the result of 64 government agencies prioritizing collaboration and encouraging information exchange.[109] The SingPass model was also recreated for businesses via the newly created CorpPass.[110] It is now used extensively to enable digital transactions across the island.

  For instance, access and use of SingPass has been extended to the Singapore Exchange (SGX) to authorize transactions requiring a high level of security for the Central Depository (CDP) services, [111] and as part of the e-signature push enabling, for example, digital signing of property caveats. During COVID-19, it was used to enable SafeEntry, a digital check-in system (that uses QR codes to 'check-in' to locations).[112] The National Digital Identity (NDI) initiative was announced in 2018 to update and upgrade the capabilities of the SingPass. It will feature three main components: biometric elements, encryption, and open application programming interfaces (APIs[113]).[114] NDI aims to give citizens digital access for secure online transactions for e-government and private sector services.
- **India**: Aadhaar is a biometrics-based identification system that allows single source offline/online identity verification for residents of India. The 12-digit identification number is used as a primary identifier to roll out government welfare schemes, and promotes transparency, hassle-free people-centric governance, and social and financial inclusion.[115] Due to its open API layers—known as 'India Stack'—Aadhaar is the foundation upon which

[108] World Bank (2021) Principles on identification for sustainable development: toward the digital age, https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf
[109] GovTech (2016) Singpass Factsheet, www.tech.gov.sg/files/media/media-releases/2016/01/SingPass%20Factsheet%20%20Updated%2029%20Janpdf.pdf
[110] GovTech (2017) Singapore Corporate Access (Corpass) Factsheet, www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/licensing/online-services/annexa-corpass-factsheet-18-dec-2017.pdf?la=en
[111] Business Times (2020) SGX's CDP offers SingPass access to authorize transactions, www.businesstimes.com.sg/companies-markets/sgxs-cdp-offers-singpass-access-to-authorise-transactions
[112] SafeEntry (2020) SafeEntry, www.safeentry.gov.sg
[113] Singpass (2021) Singpass API, https://api.singpass.gov.sg
[114] GovInsider (2017) Details: Singapore's new digital identity scheme, https://govinsider.asia/digital-gov/singapore-trials-new-digital-identity-scheme
[115] Unique Identification Authority of India (2019) Homepage, https://uidai.gov.in

an entire ecosystem of identity-driven digital transactions is being built, including digital signatures, instant payment infrastructures, and other digital government services.[116]

- **Estonia:** Estonia has built a digital ecosystem where 99% of government services have moved online. This digital ecosystem has two foundations: electronic identification (eID) and X-Road. eID is built into the Estonian identity card, which was first issued in 2002 and is a mandatory identity document for Estonian citizens. Besides regular identification purposes, the card can also be used to establish one's identity in electronic environments. At present, 99% of Estonian residents are in possession of an identity card.[117] X-Road is a centrally managed distributed Data Exchange Layer between information systems. In practical terms, X-Road is the system that allows all databases to seamlessly interact with one another, without a central server. X-Road allows information systems to function as an integrated whole, even though the architecture is decentralized.

Key takeaways

- Digital identification systems perform similar roles to identification cards, but act as an 'upgrade' on these in a variety of ways.
- Digital identification systems have the potential to streamline public and private services, making them more cost-effective and secure, whilst expanding inclusion and promoting economic growth. Designing the systems in such a way as to make them interoperable with other identity systems will enhance the potential for economic growth.
- The systems work most effectively when there is a strong already-existing digital infrastructure, as well as effective legal frameworks such as personal data and privacy legislation that meets international standards. They are also must effective when implemented in a manner sensitive to groups who are unable to share some biometric identifiers, such as people with disabilities.
- Governments should consider guarding against overreach through these systems; users should retain a degree of control over the accumulated of biometric data.
- The systems require maintenance over time and should be appropriately funded to keep them secure and effective.

[116] The Hindu (2017) Towards a unique digital South Asian identity, www.thehindu.com/opinion/op-ed/towards-a-unique-digital-south-asian-identity/article18410579.ece

[117] e-Estonia (2017) A digital success story: the cornerstone of e-Estonia celebrates its jubilee, e-estonia.com/a-digital-success-story-the-cornerstone-of-e-estonia-celebrates-its-jubilee

2.2.2 Data Sharing

What is the issue?

Data sharing has come to specifically refer to the ability to safely and efficiently access, use, and reuse data or data results. This includes the publication of open government datasets online by governments, but also includes data sharing among businesses and across economies. Data sharing has come to be seen as an increasingly integral aspect both of successful next-generation digital government development, and meaningful private sector digital transformation.

Access to abundant sources of usable data at a whole-of-government level is seen as an important enabler for the implementation of more innovative and responsive services and is understood to be a factor that can significantly affect the efficiency and efficacy of cross-agency collaboration within and between economies. Facilitating access to ample data reservoirs for the private sector by way of opening access to government data is furthermore seen as an important levelling mechanism, potentially evening out market imbalances which would otherwise endow private entities that control significant proprietary data resources with disproportionate market power.

Why is it an issue?

Data is and will continue to be the lifeblood of the digital economy. Access to data—and the development of interoperable systems, platforms, and processes for the sharing of data—thus has implications across the public and private spheres, and in all economic sectors. Limitations in access to data can, furthermore, have negative effects on the utility, relevance and inclusivity of data-related products produced using insufficiently substantive pools of data. This can in turn disadvantage economies or communities whose economic, methodological, or even cultural specificities are not represented within more widely available datasets.

Government and commercial entities alike have thus perhaps understandable developed a misapprehension of data access as being a zero-sum game, with data itself being a vital resource that must be protected and hoarded.

This zero-sum mentality has handicapped collaboration by governments and businesses within and across economies on data sharing frameworks. This perspective is arguably reflected in existing formal data sharing agreements, which tend to specify data controllers as those who provide the data, the data gatekeepers who receive, store, and manage who has access to the data, the data processors who perform the data analysis, and the data publishers who abide by the Intellectual Property Rights outlined in the agreement.

The rigidity of this approach has lent itself to constraints on access to significant datasets to large entities which are able to underwrite the procedures necessary to navigate the relevant legal and methodological barriers to entry. As applications for such datasets grow more diverse, however, it has become more important than ever to understand that data access need not be a zero-sum game, and that restricted access to data resources serves only to disadvantage all parties involved.

A growing recognition of the shortcomings of this approach has prompted more governments and businesses to adopt more fundamentally open approaches to data sharing, which aim to maximize access to promote innovative use cases and economic dynamism, while maintaining rigorous standards of trust. Nascent data sharing initiatives are accordingly in place within many APEC economies across the region and will only continue to grow in scale, complexity, and number, given the continuing expansion of the global data economy.

There is thus a need for governments to, beyond recognizing the importance of data sharing, also learn from and communicate with their counterparts in other economies to ensure that the core principles of interoperability and access are upheld, and that maximum benefit can be derived from such initiatives across different jurisdictions.

What are some considerations and challenges?

While data sharing initiatives can have a significant effect on economic integration within individual economies and across regions, , a major barrier is the lack of concerted engagement and exchange at an early stage, especially in standardizing principles and formats of data exchange. This is because accepted data formats or channels of exchange would not be interoperable or even readable across jurisdictions, limiting the degree to which separate jurisdictions are able to access and collaborate on data-related challenges using appropriately diverse and inclusive datasets.

Such a lack of regional approaches to data sharing can thus present first movers with a challenge, given the potential need to double-back on progress made if divergent regional approaches are adopted. Policymakers in such economies may seek to avert this by referring to relevant global standards and frameworks to inform economy-level efforts. Relevant standards may include ISO/IEC 38505 for data governance and ISO27701 for privacy and information management.[118] Alternatively, frameworks such as the FAIR principles for scientific data management and stewardship or the Open Contracting Partnership's Open Contracting Data Standard can be useful touchstones.[119]

Contractual issues present further difficulties, as different jurisdictions may promote unique contractual templates which may not be recognized in other jurisdictions, limiting the degree to which different governments and businesses can share and use data across economies.

There is a spectrum of data sharing arrangements, ranging from confidential bi-lateral and multi-lateral agreements to semi-open and open-data agreements, each involving either private or public parties or both. The more parties involved, the more complex agreements need to be to consider the separate interests of all the parties, and the more challenging it is to establish trust across all the parties—which is fundamental to all successful data sharing arrangements. Efforts need to be made early on to standardize contractual formats and establish common contractual frameworks for data

[118] International Organization for Standardization (2017) ISO/IEC 38505-1:2017, www.iso.org/standard/56639.html
[119] Go-FAIR (2021) FAIR Principles, www.go-fair.org/fair-principles; Open Contracting Partnership (2021) Open Contracting Data Standard, https://standard.open-contracting.org/latest/en

sharing at a regional level, both to aid in the uptake of data sharing arrangements by developing economies, and to prevent first movers from needing to duplicate work.

The diversity of data sharing arrangements is also growing significantly. There has been a gradual recognition of the degree to which data sharing alone is insufficient to the needs of both public and private sector data users. Discussions have shifted towards the need for more targeted approaches to data sharing which, instead of simply prioritizing the availability of data, also assess the specific use cases of data and therefore the most important technical and practical parameters to consider when crafting data sharing agreements.

With most currently extant government initiatives being intended to address the fundamental lack of frameworks for facilitating data sharing, policymakers can begin to consider more specific implementations of data sharing, either in the context of inter-agency collaboration or through cooperation with the private sector.

Examples of emerging practices

- **Singapore** has implemented a Trusted Data Sharing Framework to help businesses establish a baseline "common data sharing language", reflected in the circulation of Data Sharing Agreement, Confidentiality Agreement and Data Subject Consent templates.[120] This Framework was also accompanied by the Data Collaboratives Programme (DCP), which is designed to support efforts by businesses to design and implement mechanisms for the safe and economically sustainable sharing of data.[121] The DCP furthermore integrates a Data Regulatory Sandbox mechanism by which businesses and data partners are able to design and pilot innovative data use cases while reducing uncertainties with regards to regulatory or compliance obligations, in consultation with the Infocomm Media Development Authority (IMDA) of Singapore and Personal Data Protection Commission (PDPC).
- **Australia's** Data Availability and Transparency Bill 2020 introduces data reforms that will modernize and streamline how the govt uses and shares data between agencies and with the private sector and academia.[122] The bill along with the Data Availability and Transparency (Consequential Amendments) Bill creates a scheme of controlled access to public sector data. Data will be shared for the purposes of public sector services delivery, informing govt policy and programs, and R&D.
- **Thailand** passed the Digitalization of Public Administration and Services Delivery Act B.E. 2562 (2019), or the Digital Government Act, in 2019. [123]The Digital Government Act outlines detailed parameters determining the rights, duties, and responsibilities for the management of data by State Agencies. This notably includes stipulations that government agencies are to digitalize data under their missions and ensure that data is complete, credible, correct, current and both shareable and usable by other government agencies, including for the

[120] IMDA (2019) Trusted Data Sharing Framework, www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf
[121] IMDA (2020) Data Collaboratives Programme, www.imda.gov.sg/programme-listing/data-collaborative-programme
[122] Parliament of Australia (2021, Data Availability and Transparency Bill 2020, www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6649
[123] Digital Government Development Agency (2019) Digital Government Act, www.dga.or.th/wp-content/uploads/2021/02/6.pdf

purposes of further processing. The Act further contains language laying the groundwork for the establishment of an agency with the mandate of gathering and collating data from across different agencies, by making cooperation and interconnectivity with such an agency mandatory for all other state agencies.

- **Viet Nam** has linked the National Public Service Portal (NPSP) to the economy's insurance database, and citizens are now able to access different services such as payments for voluntary social insurance.[124]
- **Digital Economy Partnership Agreement (DEPA)** signed by Chile; New Zealand; and Singapore introduces specific articles recognizing the need to facilitate public access to and use of government information for the fostering of development, competitiveness, and innovation.[125] The DEPA asserts the commitment of signatories to ensuring that government data is made available to the public as open data, and signals a further commitment to collaboration within and across economies to identify sectors where open data sets with "global value" can be used to facilitate technology transfer, talent formation and innovation.

Key takeaways

- Data sharing has come to be recognized as an increasingly vital driver of the digital economy, with implications on the efficiency and efficacy of government services, as well as the competitiveness of private sector offerings.
- Data sharing can deliver benefits for key industry sectors like digital financial services, health services, education and for better policymaking and planning in areas such as housing and transportation.
- At the same time, challenges remain regarding the acceptance of data sharing, due to entrenched attitudes towards the proprietary nature of data, and perceptions of the data economy as a zero-sum game.
- The uneven shift towards data sharing creates the possibility that divergent standards of data formatting or storage may be adopted across different jurisdictions, which would hamper interoperability in the long run.
- There is additionally a growing awareness of the limitations of passive data sharing approaches, and a gravitation towards more targeted approaches to data sharing which emphasize specific objectives and use cases for shared data.

[124] National Public Service Portal (2020) Notice from July 1, 2020, https://dichvucong.gov.vn/p/home/dvc-chi-tiet-tin-tuc.html?new_id=501

[125] Ministry of Trade and Industry, Singapore (2021) Digital Economy Partnership Agreement, www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement

2.2.3 Quality of Service (QoS)

What is the issue?

The International Telecommunications Union (ITU) defines Quality of service (QoS) as the "totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service".

QoS standards and reporting requirements can be specified as part of the licensing criteria for a service operator, such as a telco, ISP or broadcaster. These may be deemed to be particularly important where, for example, emergency services access is a consideration. QoS performance indicators serve as a means for regulators to assess the performance of traffic on an operator's network and protect consumer interests by ensuring that services meet minimum prescribed standards.

Common parameters used to measure broadband QoS include data transmission speeds, network availability/coverage and network latency. Some economies impose QoS standards on ISPs as part of license conditions, regulatory requirements or industry guidelines, whereas some rely on market forces to determine QoS if there is sufficient competition.[126]

Why are QoS requirements an issue?

Spikes in data traffic volumes and unanticipated changes in consumption patterns can result in operators facing difficulties in meeting their QoS obligations. There is an argument that a growing demand for high-bandwidth online services, such as streaming video-on-demand, have contributed to ISPs' and telcos' cost burden, and in some cases, impede on their ability to fulfil QoS requirements.

In addition, because the quality of Over-the-Top (OTT) services depends heavily on the underlying broadband services provided by ISPs and telcos, OTT providers that generate the most data traffic should therefore be obliged to share the cost of maintaining, expanding or upgrading the networks they use to deliver their content.

This became a particular challenge through the COVID-19 pandemic as network demands jumped as more people were using online services and governments were compelled to respond to ensure that citizens were able to continue to work, learn, and play. Being depended upon by governments, communities and businesses to provide what is now considered an essential service for economic and social activities to continue amid lockdowns, telcos and ISPs are struggling to cope with the financial costs of having to make unexpected network management investments to handle surging Internet traffic whilst delivering QoS.

---

[126] International Telecommunication Union (2017) Quality of service regulation manual, www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.QOS_REG01-2017-PDF-E.pdf

With no globally accepted best practice on how these costs should be shared, and insufficient research into the actual effectiveness or possible consequences of such measures, regulations that seek to hold OTT providers liable for the quality and reliability of networks run the risk of undermining policies on net neutrality and competition, and create issues for consumer choice and enforcement.

What are some considerations and challenges?

The issue had already been causing ongoing tension in recent years with the success of digital services and, in particular, the rapid rise of OTT services, leading to some domestic telcos, ISPs and broadcasters pushing back through various means for 'contributions' of one sort or another to be placed on the larger OTT service providers.

However, QoS is being used by various jurisdictions to address a set of issues variously encompassing net neutrality, digital competition, consumer choice, content moderation, and promotion of the digital economy—all on the basis of cost reallocation.

For example, in Korea, a revision to the Telecommunications Business Act was passed in May 2020, mandating OTT service providers that account for more than 1% of the economy's domestic Internet traffic, and have an average daily user count of 1 million or more over a three-month period to negotiate QoS agreements with telcos.[127]

However, as what constitutes sufficient mitigation and efforts to maintain QoS levels has not been clearly defined, the revision is largely seen as a measure to force foreign OTT companies to share network costs with telcos and ISPs, and may open doors to opaque processes and anti-competitive practices, which could result in distorted markets where: i) dominant telcos abuse their disproportionate bargaining power and charge excessive prices for content delivery; and ii) dominant OTT providers collude with telcos to set unrealistic QoS conditions that drive their competition out of the market. Consumers will suffer at the consequence of anti-competitive markets.

An additional problem is that when the QoS responsibility quality is shared, it becomes difficult to arrive at an exact and objective definition of what is an acceptable or appropriate level of contribution by telcos, versus that of OTT providers (of which there may be multiple, with varying levels of profitability and market share). This ambiguity may create complications when QoS issues arise.

Moreover, there is a high likelihood that the new costs OTT providers are forced to bear will be passed on to domestic consumers, essentially charging them twice for broadband services—directly through their home and mobile subscription fees, and indirectly through the additional compliance costs passed on from the OTT provider.

---

[127] Ministry of Science and ICT (2020) Amendment to the Enforcement Decree of the Telecommunications Business Act, www.msit.go.kr/SYNAP/skin/doc.html?fn=e3d5a760c6459a07f4efe530141ddbfe&rs=/SYNAP/sn3hcv/result/

Examples of emerging practices

Instead of imposing QoS obligations which may result in ambiguity around the scope of OTT providers' responsibility, higher consumer costs and even anti-competitive practices, maintaining flexibility and responsiveness in regulatory approaches has also been key to delivering agile and appropriate responses to QoS concerns during the COVID-19 period.

- **Europe**: SVOD providers were asked to temporarily adapt their throughput by reducing high-definition video quality to standard definition to alleviate network congestion. This was deemed to be an exceptional traffic management measure according to the EU Open Internet Access provisions,[128] which allowed broadband QoS issues to be addressed without the need to impose new regulatory requirements on OTT/SVOD providers.

Key takeaways

- Regulators should take a responsive and flexible approach to emerging QoS issues, and should work closely with industry to arrive at the approach that will be most appropriate for achieving its objective.
- The responsibility for managing network costs and performance should lie with the network operator and should not be imposed on OTT providers as a condition to deliver their services over the open Internet.
- Network operators already collect data usage fees from end users, and imposing the same on the other side of the market (i.e., OTT providers) will lead to consumers paying higher prices for the same services, since the duplicated fees levied on OTT providers will most likely be passed on to consumers.
- When considering the OTT industry's impact on broadband QoS, regulators should also recognize their contribution to non-telco/ISP owned network infrastructure, such as Content Delivery Networks (CDNs), that support the network backbone.

[128] European Commission (2020) Commission and European regulators calls on streaming services, operators and users to prevent network congestion, https://ec.europa.eu/digital-single-market/en/news/commission-and-european-regulators-calls-streaming-services-operators-and-users-prevent-network

2.3 Emerging Issues

2.3.1 Artificial Intelligence (AI)

What is the issue?

Artificial intelligence (AI) is the general catch-all term—often misused—for computing systems that emulate human cognitive functions, such as identifying patterns to solve problems, and comprises machine learning, deep learning, big-data analytics, augmented intelligence, automation, and some types of robotics.

AI is rapidly becoming central to the global economy. A variety of different forms of AI are being introduced across sectors, industries, and widely across society, contributing to the economic dynamism of both emerging and mature economies across the APEC region.

For businesses, AI provides immediate potential productivity gains—enabling the automation of tasks, the streamlining of processes, and the optimization of resources—and can create long-term competitiveness by boosting overall investment and innovation. AI is expected to continue transforming a range of industries and creating new, previously unforeseen occupations, products, and services.

For governments, AI can help address a range of issues, including complex and longstanding socio-economic challenges such as poverty and vulnerability to natural disasters.[129] If used as a full-fledged priority and not just as a productivity tool, AI can accelerate digital trade, enable smart cities,[130] address environmental challenges,[131] and transform global resilience in times of crisis. For example, AI can help economies tackle challenges created by COVID-19, including long-term economic consequences.[132]

Why is it an issue?

The combination of vast amounts of data, cloud computing power, and improvements in Internet connectivity are driving rapid improvements in AI technologies. This, coupled with growing recognition that applying AI to the data available to them can enhance almost any business process by bringing additional insights and intelligence to bear, is driving the application of AI across all sectors of the economy and it is widely accepted that AI will have a transformational effect on future economic development and growth.

---

[129] UNDP (2019) Using AI to help achieve Sustainable Development Goals, www.undp.org/content/undp/en/home/blog/2019/Using_AI_to_help_achieve_Sustainable_Development_Goals.html
[130] Nvidia (2021) Smarter cities through AI, www.nvidia.com/en-us/industries/smart-cities
[131] National Geographic (2019) How artificial intelligence can tackle climate change, www.nationalgeographic.com/environment/2019/07/artificial-intelligence-climate-change
[132] Forbes (2020) How artificial intelligence can help fight coronavirus, www.forbes.com/sites/cognitiveworld/2020/03/19/how-artificial-intelligence-can-help-fight-coronavirus/#33a275634d3a

Tools founded on and enabled by AI, such as AI algorithms, have come to the fore, due in part to how they have fueled the success of digital platforms. AI allows marketing campaigns to be more targeted without substantial research cost, and helps improve customer satisfaction and therefore long-term retention. It has been argued, for example, that the real value of Netflix lies not in its content library, but in its recommendation engine, which is effectively able to serve as a market research tool, marketing campaign platform and customer retention program.[133] Similarly, Amazon, eBay, and Alibaba have grown their businesses based on sophisticated recommendation and customer-insight engines.

Because both the applications and understanding of AI are still developing, policy frameworks continue to be in early stages. A key factor underlying regulatory concerns is the lack of transparency surrounding AI algorithms,[134] including how they collect and process data and how this translates into service provision from digital platforms.

In an attempt to pull the curtain back on opaque AI practices and to address the potential negative ramifications such as price discrimination and profiling, regulators may be tempted to overregulate instead of opting for more nuanced approaches. This could result in obtrusive measures such as revealing source code that could serve to disincentivize the use of innovative technology, or putting in place restrictive policies (such as local server requirements or consent provisions for each use of data) that limit innovation.

What are some considerations and challenges?

Policymakers have shared concerns in the understandability of AI, and see the importance of developing ethical and responsible AI. The complexity of deep learning techniques means that unstructured data enters a black box, and the algorithm makes predictions or decisions without human intervention. Without explanation about what factors led to the decision and how it occurred, challenges arise where the decisions have corresponding societal implications (i.e., social justice systems, hiring decisions, financial lending).[135]

With the vast amounts of data fed into the black box to train the algorithm, biases and discrimination may be introduced at the onset via the seemingly innocuous selection of data, which may end up not being representative of the population, thus further replicating and embedding biases that already exist. Further, just because an algorithm has run through the decision-making process, could mistakenly lend a veneer of scientific credibility to reinforce that final decision.

---

[133] Association for Computing Machinery (2016) The Netflix recommender system: algorithms, business value, and innovation, https://dl.acm.org/doi/10.1145/2843948

[134] Bureau Européen des Unions de Consommateurs (BEUC) (2018) Ensuring consumer protection in the platform economy, www.beuc.eu/publications/beuc-x-2018-080_ensuring_consumer_protection_in_the_platform_economy.pdf

[135] Harvard Business Review (2016) A guide to solving social problems with machine learning, https://hbr.org/2016/12/a-guide-to-solving-social-problems-with-machine-learning

For the widest adoption of AI, people must have confidence they can trust the technology. Industry and governments recognize there is uncertainty as to how AI will reflect ethical values. Ethical AI development and responsible AI use have emerged as key concerns, particularly as more AI-enabled devices, platforms, and services leverage citizens' and consumers' data.[136]

A majority of APEC member economies already have a plan, policy, or program specifically devoted to driving or supporting AI ecosystems. While their approaches differ, they generally strive to stimulate AI development to the benefit of their economy, while preparing society for the potential changes that may be brought about by AI. AI is an area where the risk of divergent policy and regulatory approaches is poignant, which can threaten regional economic growth and trade since AI is a technology that is increasingly becoming embedded into business processes, products and services.

As further investments are poured into acquiring more data and capabilities, the gap between the early adopters and laggards may widen.[137] The same may also occur in developed economies that have the ability to invest in advancing AI, and also drive a bigger divide in future GDP growth and the digital divide between them and other developing economies.[138]

AI is expected to be the most broadly adapted technology across digital information and communications, online recruitment, digital financial services, healthcare, and transportation industries by 2025. It is important to note that economies with high wages that see more of the workforce involved in pattern-oriented or predictive work will likely be disrupted by automation more than economies with lower wages—as it will be a slower shift to deploying higher cost AI technology. Jobs that require repetition, structure and data processing will be most adversely affected by AI, while those that require human touch (and that are difficult to automate) will flourish. There could also be a shift to social and emotional skills such as communication and empathy being demanded.

Examples of emerging practices

To address growing concerns about the safe, ethical, responsible, and unbiased use of AI—particularly as more AI-enabled devices, platforms, and services leverage consumer data—a number of regional frameworks, and sector-specific frameworks (focused initially on financial data and consumer protection) have emerged. Many of these use a principles-based approach which provides businesses with an understanding of the government's expectations while still giving space for use of innovative technology.

---

[136] Forbes (2018) Can AI be trusted with life and death decisions?, www.forbes.com/sites/forbestechcouncil/2018/02/16/can-ai-be-trusted-with-life-and-death-decisions/#5e361e845951
[137] McKinsey Global Institute (2018) The promise and challenge of the age of artificial intelligence, www.mckinsey.com/featured-insights/artificial-intelligence/the-promise-and-challenge-of-the-age-of-artificial-intelligence
[138] ITU (2018) Assessing the economic impact of Artificial Intelligence, www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-ISSUEPAPER-2018-1-PDF-E.pdf

- **Europe:** European Commission is proposing its first ever legal framework on AI, to ensure AI systems are safe and respects existing law, ensure legal certainty to facilitate investment in AI, enhance governance and enforcement of law and facilitate development of a single market for trustworthy AI.[139]
- **OECD:** Members have signed up to the OECD Principles on Artificial Intelligence, to provide guidance in designing and running trustworthy AI systems that places people's best interests at the heart.[140] This ensures that the systems are robust, safe, fair and trustworthy.
- **Singapore:** It has drafted a Model AI Governance Framework establishing two key principles, that AI decision making be explainable, transparent, and fair, and that AI solutions be human-centric, for organizations to use AI responsibly and ethically. The Framework further lays out guidance in areas such as internal governance, the level of human involvement in AI decision making, and operations management.[141] In the finance sector, the Monetary Authority of Singapore (MAS) has also released fairness, ethics, accountability, and transparency (FEAT) principles for the use of AI and data analytics which similarly provide internal governance guidance for institutions providing financial services.[142] The AI Singapore program was also launched to enhance AI capabilities, drive investment, and expand adoption.[143]
- **Australia**: The government has developed a cross-cutting AI Ethics Framework, including a set of voluntary AI ethics principles which focuses on goals such as fairness, privacy protection, reliability, and transparency.[144] The Human Rights and Technology Report sets out the Australian Human Rights Commission's proposed roadmap for responsible innovation,[145] and the Artificial Intelligence Standards Roadmap sets out a proposed approach to ensure Australia can effectively support AI standards development internationally.[146]
- **Singapore-Australia Digital Economy Agreement:** The bilateral digital trade agreement includes an MoU to cooperate on AI capabilities, new AI technologies, talent development

[139] European Commission (2021) Regulation of the European Parliament and of the Council – laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[140] OECD (2019) Forty-two countries adopt new OECD Principles on Artificial Intelligence, www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm

[141] Personal Data Protection Commission (PDPC) (2020) Model Artificial Intelligence Governance Framework Second Edition, www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

[142] Monetary Authority of Singapore (MAS) (2018) Principles to promote fairness, ethics, accountability and transparency (feat) in the use of artificial intelligence and data analytics in singapore's financial sector, www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat

[143] National Research Foundation (NRF) (2017) AI.SG: new national programme to catalyse, synergise and boost singapore's artificial intelligence capabilities, www.nrf.gov.sg/docs/default-source/modules/pressrelease/201705031442082191-press-release-(ai.pdf

[144] Department of Industry, Science, Energy and Resources (2021) Australia's Artificial Intelligence Ethics Framework, www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework

[145] Human Rights and Technology (2021) Human Rights and Technology Final Report, https://tech.humanrights.gov.au/downloads

[146] Standards Australia (2020) An artificial intelligence standards roadmap: making australia's voice heard, www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspx

and ethical standards to foster the positive commercial applications of AI in the digital economy.[147]

Key takeaways

- AI is transforming businesses and governments, improving efficiencies, reducing costs, and enabling innovative products and solutions, across all sectors of APEC member economies resulting in broad economic growth and development. AI is neither just a technology issue nor a governance concern; increasingly it is becoming a central feature for economic growth and promotion of digital trade across APEC. Recognizing the economic impact and potential of AI, and therefore ensuring that AI policies are beneficial in advancing that growth within APEC, is a key priority for economic cooperation and development across the region.
- While AI is new and presents a host of opportunities, such opportunities will only come to fruition if citizens, businesses, and governments are comfortable adopting and using the applications that are deployed. Citizens not only need confidence that AI is being deployed in a safe, responsible, and accountable manner, they need to be able to enjoy and benefit from the experience on an ongoing basis. Data-driven innovations, products, and services need to be developed and deployed in an ethical, and trustworthy manner.
- Governments have a key role to play in developing enabling AI ecosystems (expanding and ensuring access to digital infrastructure, investing in research and innovation, access to data including open government datasets, and supporting start-ups) and enabling policy and regulatory frameworks that balance innovation with safety and integrity. This includes identifying supportive policies (including inclusion and accessibility considerations) across a range of areas, including privacy (and clarity for text and data mining), data flows, IP protection, and cybersecurity.
- As with other cross-jurisdictional networked technologies (e.g., cloud computing), a harmonized regional position on principles and standards will ensure that all APEC member economies benefit from the sophistication and proliferation of AI. Efforts towards minimizing the operational, compliance, and financial costs of adopting AI systems across different jurisdictions through internationally aligned frameworks and standards—enabling data to move across borders, data to be leveraged from multiple jurisdictions to improve AI, or to use the same AI product or service across multiple economies—will increase commercial benefits of scale and business opportunities.
- As strategies continue to develop, economies will need to consider how best to address emerging skills requirements, and effectively re-skill workers to ensure the benefits of AI are shared as widely as possible.

[147] DFAT (2020) Australia-Singapore Digital Economy Agreement: summary of key outcomes, www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-summary-key-outcomes

2.3.2 Intermediate Liability

What is the issue?

Intermediary liability describes the allocation of legal responsibility to digital content and service providers of all kinds of regulated categories of content.[148] The topic of intermediary liability is closely interlinked with the issues of IP and content moderation, since it involves defining the extent of legal liability digital platforms are subject to for the actions of their users. This is 'secondary' or 'indirect' liability as it does not relate directly to the intermediary's own conduct.

At its broadest definition, intermediary services can include: [149]

- Network infrastructure, such as ISPs;
- Online marketplaces that provide access to goods and/or services offered by third parties (e.g., bringing together and facilitating transactions between merchants and consumers), such as Alibaba, Amazon, and Lazada;
- Digital platforms that bring together providers and consumers offering material services (or 'sharing' of resources), such as Grab, Go-Jek, Uber, and Airbnb, or access to a workforce, expertise, or labor tasks, such as AirTasker, and TaskRabbit;
- Platforms that provide access to money or capital, including crowdfunding sites such as Kickstarter and Gofundme, and payment systems such as PayPal, Mastercard, Visa, and Bitcoin;
- Aggregators that provide access to information or content, including:
    - Search engines such as Google or Bing;
    - Video platforms, such as YouTube;
    - Social networks, such as Facebook;
- Online hosting services including cloud computing services, such as Amazon Web Services, Microsoft Azure, and webhosting services and storage services, such as DropBox.

Discussions on determining where liability rests and the extent of intermediary liability are focused on intermediary service providers who provide a mere conduit, caching, or hosting service (e.g., holding Facebook accountable for user-generated content published on their feed). These services to date have enjoyed a so-called 'safe harbor' regime, and have avoided liability for harmful or illegal activities performed by their users. Discussions focus on large digital platforms, such as Facebook, but all online services—from large tech companies to small, independent websites—have benefitted from intermediary liability provisions.[150]

---

[148] Global Network Initiative (2021) Intermediary Liability, https://globalnetworkinitiative.org/policy-issues/intermediary-liability-content-regulation

[149] Nataliia Filatova-Bilous (2021) Once again platform liability: on the edge of the 'Uber' and 'Airbnb' cases, https://policyreview.info/articles/analysis/once-again-platform-liability-edge-uber-and-airbnb-cases

[150] ITIF (2021) Overview of Section 230: what it is, why it was created, and what it has achieved, https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved

Why is it an issue?

Intermediary liability protections ('safe harbor') have been fundamental to the growth of the open Internet, providing a safety net that allows digital intermediaries to operate with the certainty that they will not be legally liable for storing, hosting, processing, or transmitting content, since the flipside of that is that digital intermediaries face higher legal risks that they will try to mitigate through early or unnecessary blocking of content or censorship.

Section 230 of the United States' Communications Decency Act,[151] is a set of policies passed in 1996 that provided protection of the Internet and innovation—known as a safe harbor. Section 230 states digital platforms (dubbed "interactive computer services") cannot be treated as the publisher or speaker of third-party content, and has two key subsections that govern user-generated posts:

- The first—section 230(c)(1)—means that almost all user-generated content posted on a platform's website will not create legal liability for the platform even if the post is defamatory, dangerous, abhorrent, or otherwise unlawful (noting there are exceptions for copyright violations, sex-work related material, and violations of federal criminal law); and
- The second—section 230(c)(2) allows platforms to police their sites for harmful content, but it does not require that they remove anything, and it protects them from liability if they choose not to.

Section 230 acknowledged and preserved the early principles of the Internet—that infrastructure providers were seen as 'dumb pipes', merely transferring or hosting data, and could not be responsible for blocking objectionable content.[152] This concept enabled the Internet to grow, encouraged uptake and innovation in online services, and protected digital platforms from regulation and liability that might impede those goals.[153]

However, today these digital platforms are bigger, engaged in more activities, and offer more services—and have unwittingly turned into developers, disseminators, and amplifiers of potentially harmful and illegal content. There is a growing consensus that Section 230—and the concept of intermediary liability—needs to be re-examined.

What are some considerations and challenges?

While the definition adopted by economies and their liability regimes vary considerably across the region, most have adopted a conditional liability regime that exempts an intermediary from liability on the condition that it adopts certain measures or policies, such as the take-down of IP infringing,

[151] US House of Representatives (2021) 47 USC 230: Protection for private blocking and screening of offensive material, https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)
[152] Internet Society (2020) Intermediary liability: the hidden gem, www.internetsociety.org/blog/2020/03/intermediary-liability-the-hidden-gem
[153] *Ibid.*

defamatory, or otherwise illegal content. Approaches to intermediary liability adopted by APEC member economies include:

- **Actual knowledge:** Australia,[154] Japan,[155] and the Philippines[156] adopt provisions setting out that digital platforms are only accountable for content they are aware of or have 'actual knowledge' of.
- **Notice and takedown:** New Zealand[157] adopts provisions requiring online services must follow notice and takedown requests for content that is deemed unlawful. The United States[158] adopts this approach for online intermediary liability for copyright, where the copyright owner may send a notice of copyright infringement to an Internet intermediary, and the Internet intermediary must then 'expeditiously' disable access to, or remove, the content in question

At present, several advanced economies are considering introducing legislation that requires companies to make 'reasonable best efforts' to remove illegal content, marking a departure from current regulations that permit businesses to seek out and remove illegal content without rendering them liable for any such content that they still store or process.

It must also be noted that many of the concerns about digital platforms—spread of misinformation and offensive content and the power of social media to prevent or promote such communication—is a function of their scale and augmented network effects. These same network effects that have spread hate speech, have also benefited users through social movements such as the Arab Spring, #MeToo, and #BlackLivesMatter.

Examples of emerging practices

- **Europe:** The Digital Services Act proposes reforms to intermediary liability protections, placing more responsibilities on online intermediaries to protect users. The proposal takes a four-tiered approach with cumulative obligations for intermediary service providers, hosting service providers, online platforms, and very large online platforms. Most obligations apply to the latter two categories. Intermediary service providers—mere conduit, caching and hosting—will be subject to possible orders from domestic authorities to remove illegal content, transparency reporting, information requirements for their terms and conditions, and be required to appoint a point of contact or legal representative. Hosting service

[154] Federal Register of Legislation (2021) Broadcasting Services Act 1992 (Commonwealth of Australia), Schedule 5, Clause 91, www.legislation.gov.au/Details/C2021C00042
[155] UNESCO (2001) Act on the limitation of liability for damages of specified telecommunications service providers and the right to demand disclosure of identification information of the senders (Japan, 2001), Article 3, Clause 1, www.unesco.org/culture/pdf/anti-piracy/Japan/Jp_%20LimitLiability_Telecom_en
[156] The Official Gazette (2000) An Act providing for the recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof, and for other purposes (Republic of the Philippines, 2000), Section 30, www.officialgazette.gov.ph/2000/06/14/republic-act-no-8792-s-2000/
[157] Parliamentary Counsel Office (2015) Harmful Digital Communications Act 2015, Section 6, www.legislation.govt.nz/act/public/2015/0063/latest/whole.html
[158] U.S. Copyright Office (1998) The Digital Millennium Copyright Act of 1998, www.copyright.gov/legislation/dmca.pdf

providers will be subject to additional obligations including implementing a notice and action mechanism and issuing statement of reasons.[159]

Key takeaways

- Safe harbors have supported the emergence of innovative services, providing intermediaries with the sufficient legal certainty to conduct a wide range of activities, free from the threat of potential liability and the chilling effect of potential litigation.
- However, there is a growing consensus that we need to update intermediary liability concepts to take into account the cost and scope of harm of user-generated content, and a duty-of-care approach—ensuring digital platforms are held accountable whilst still enabling innovation.

[159] European Commission (2020) The Digital Markets Act: ensuring fair and open digital markets, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

2.3.3 Content Moderation

What is the issue?

Content moderation refers to the practice by online platforms to screen user-generated content and ensure that the published content does not violate rules and guidelines against prohibited, illegal, or inappropriate content, such as content related to copyright infringement, child pornography, violence, or instigating violence against certain groups, hate speech, harassment, calls for terrorism, and misinformation.

Content moderation includes takedown demands, such as formal requests from governments to remove content that is deemed illegal, unlawful, or inappropriate.

Why is it an issue?

Content moderation can be a predominant issue in certain jurisdictions when rules are unclear about *what* is considered prohibited content (e.g., violence, terrorism, porn, sexualization of children, hate speech, obscene or vulgar, illegal or against religious or societal values) and *who* it applies to (e.g., OTTs, video-on-demand (VOD)/ subscription video-on-demand (SVOD) providers and user-generated content providers (UGCPs)).

Without defining clear rules and responsibilities, takedown demands become more ad-hoc, and based on what the authorities may or may not deem to be appropriate. Given the varied nature of content on digital platforms, it becomes increasingly difficult, costly, and time-consuming to comply with individual takedown demands. Across economies, there is no consensus on:

- What kind of content is considered harmful, abusive, prohibited, or illegal;
- Whether digital platforms should only remove content that has been notified to them (or whether it should be flagged by individuals or government authorities), or whether the scope should be extended to removal of content that should be 'easy' for platforms to identify themselves; and
- How governments should determine and calculate administrative sanctions, including fines, and how to enforce them.

What are some considerations and challenges?

When determining whether to hold digital platforms liable and accountable for removal of content, economies must seriously consider a number of factors, including:

- Impact on free speech and expression;
- 'Outsourcing' of decision-making regarding what constitutes illegal content to private companies; and
- Whether and how extraterritorial issues (where providers are not based in the same jurisdiction) are overcome in an effective way.

Content moderation is a complex, global issue, which cannot be easily tackled by reactive legislative instruments. Measures put in place need to be principles-based, adaptable to technological developments, and balanced as under-moderation results in the spread of harm and abuse, whilst excessive content moderation may give rise to concerns around censorship, bias, and constraints on social interactions.

Decisions regarding removal and suspension are not clear cut. Facebook has noted that they will always get some moderation decisions wrong.[160] For example, although Facebook's Oversight Board upheld its decision to restrict Donald Trump's Facebook and Instagram account access, it also indicated that Facebook's imposition of a penalty of indefinite suspension was inappropriate, and had called for it to impose a penalty in line with its normally stipulated penalties. Namely, removing violating content, imposing a time-bound suspension or permanently disabling a page and account. The Oversight Board is calling for a review of the matter within six months of the decision, and has suggested recommendations for Facebook to develop "clear, necessary and proportionate policies that promote public safety and respect freedom of expression."[161]

As the pressure steps up primarily on social media platforms, they are increasingly moving away from minimum community standards to being aggressive on policies, yet applying selective enforcement. This is seen in their development of centralized systems that entail a single set of rules, to be enforced globally. This results in is a race to the bottom, where platforms attempt to amalgamate the restrictions of economies.[162]

Digital platforms are also under time pressure to remove content quickly or face liability, leading to the incentivization of simply applying broad censorship quickly. To manage this, companies rely more on AI tools to flag and take down content. Speed is emphasized over accuracy and puts a further squeeze on the freedom of expression. For example, Twitter's algorithm was flagging tweets containing the words 'oxygen' and 'frequency' as requiring a COVID-19 fact-check even when the subject matter was completely unrelated[163]—demonstrating the limitations of leaving content moderation purely in the hands of the technological tools.

Content moderation processes also need to be localized, including regional and jurisdictional presence in order to pick up on local nuances and language considerations. For example, Facebook does not have its content reporting guidelines translated into the major languages it services, or

[160] Facebook (2020) Charting a way forward: online content regulation, https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf
[161] Oversight Board (2021) Case decision 2021-001-FB-FBR, https://oversightboard.com/decision/FB-691QAMHJ/?s=08
[162] Forbes (2018) Is social media content moderation an impossible task?, www.forbes.com/sites/kalevleetaru/2018/09/08/is-social-media-content-moderation-an-impossible-task/?sh=78534ce615fa
[163] Clifford Chance (2020) Content moderation and online platforms: an impossible problem?, https://talkingtech.cliffordchance.com/en/industries/e-commerce/content-moderation-and-online-platforms--an-impossible-problem--.html

ensures that they reflect discrimination for a regional context (such as caste), and as such, offers no appropriate options and classifications.[164]

This extraterritoriality issue is of fundamental importance. Due to the borderless nature of the Internet—where a user may upload content in one economy, to a platform operated by staff based in a different economy, with comments left by other users in a third economy—poses challenges to economies (and digital platforms) in tackling the issue.

While we are seeing examples of economies beginning to impose measures that go well beyond their borders—problematic in and of itself as such actions may impinge on the rights and freedoms of citizens in other jurisdictions—how those measures are *enforced* cross-jurisdictionally remains an open question. For example, if one jurisdiction orders a social media platform to remove content not just from their jurisdiction, but globally, Internet users in other jurisdictions may have their freedom to access information violated based on a foreign law.

Equally or perhaps more problematic is the impact such actions could have on the domestic digital economy. The general impression of content moderation is that it applies mainly to text or speech. While this may be true to a large extent, it is important to consider how access to digital platforms is central to the way we live, work, and exist in communities (e.g., food delivery, transportation, entertainment).

Examples of emerging practices

- **United Kingdom**: In 2019, the UK released a framework in an Online Harms white paper, which proposes requirements for Internet companies to ensure they keep their platforms safe and holds them accountable for the content on their platforms, as well as the decisions of the company. The proposal was for the framework to be enforced by a new regulatory body, under which companies and executives who breach the proposed statutory duty of care could be charged with hefty fines.[165] The draft Online Safety Bill defines a list of specific kinds of harmful content (some more severe than others) and creates an active obligation for consumer Internet services to try to minimize them. Where Section 230 in the USA lets companies try to remove such content without rendering them liable if their actions are deemed insufficient, the UK will require these companies to try to remove harmful content as part of their duties of care.[166]
- **Singapore:** Three key codes have been set out in its regulatory framework: i) Internet Code of Practice, sets baseline obligations for Internet services and content providers operating in Singapore; ii) Internet Regulatory Framework, provides an overview of the economy's approach to online regulation and links to the Code of Practice; and iii) The Protection from

[164] Al Jazeera (2020) For Facebook, south and southeast asia is only a market, www.aljazeera.com/opinions/2020/11/13/for-facebook-south-and-southeast-asia-is-only-a-market
[165] Gov.uk (2020) Online Harms White Paper, www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper
[166] Gov.uk (2021) Draft Online Safety Bill, www.gov.uk/government/publications/draft-online-safety-bill

Online Falsehoods and Manipulation Act (POFMA), addresses the spread of misinformation through correction and removal orders.[167]

Key takeaways

- To streamline content management and reduce inefficiencies, regulators should provide clear rules and parameters about prohibited content, taking into account the distinct differences in mediums of content delivery. This will ensure that takedown requests are minimized and only used in instances of clear violation of rules. In addition, businesses should have access to an appeals process and legal recourse in order to challenge a takedown request.
- Successful approaches clearly delineate prohibited and unacceptable content and limit the instances where notice and takedown processes have to be utilized. In parallel, notice-and-takedown processes are clearly laid out, which reduces friction between the regulators and service providers.

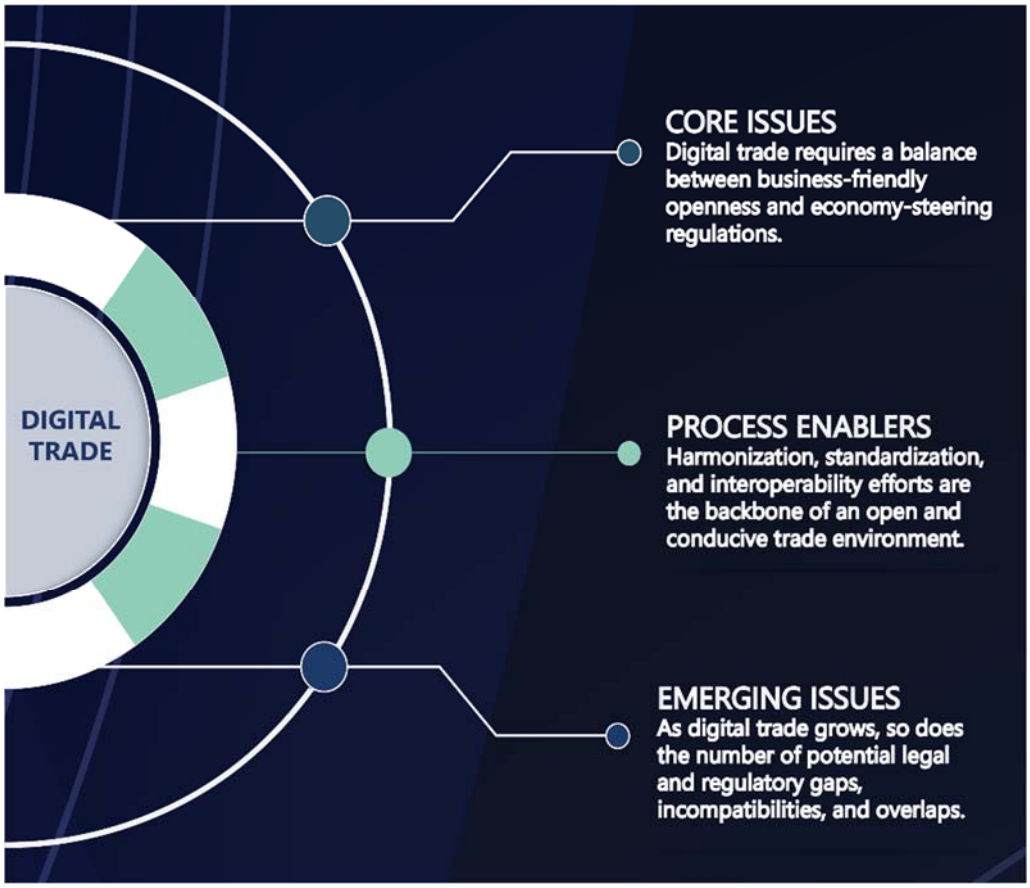
[167] Tech against Terrorism (2020) The online regulation series: Singapore, www.techagainstterrorism.org/2020/10/05/the-online-regulation-series-singapore

3. Digital Trade Issues

The globalization of the Internet and the ability to move data across borders underpins an increasing amount of economic activity and international trade. Digital technologies have transformed businesses and the way in which business is done, allowing any business to potentially reach overseas customers and sell products online. One of the major challenges currently in relation to digital trade is ensuring balance between openness, or facilitation of regional/global digital trade (e.g., limiting frictions within the system), and maintaining an economy's right to regulate for what are known as 'legitimate public policy objectives' (LPPOs).

At the heart of this challenge are three key areas to consider: **i) Issues that are core to trade flows; ii) Process enablers,** and **iii) Emerging digital trade fragmentation**. Again, these are examined separately within the Primer, but it is important to note that they function in close interconnectedness.

Figure 5: Digital Trade Issues



Source: Access Partnership (2021)

3.1 Core Issues

3.1.1 Cross-Border Data Flows

What is the issue?

Cross-border data flows refer to the movement of data across domestic borders and are key to any form of digital trade. Beyond considerations of e-commerce (from payments, products, and supply chains), this movement of data furthermore enables the use of emergent data-driven technologies such as additive manufacturing, cloud computing and AI, all of which have potential transformative effects on economic development and trade.

Why is it an issue?

Every sector—from manufacturing, healthcare, retail, finance, agriculture—relies on data and the flow of that data whether directly, or by indirectly taking advantage of tools such as cloud computing. Businesses have thrived in a global market where their services can be more easily provided and consumed, finetuned to customer preferences, and monitored and supported in real-time due to the benefits enabled by frictionless data flows.

Because many such businesses, especially smaller players, rely on globally distributed data storage and information security systems for operational cost savings, and access to tools enabled by these systems, any measures put in place to slow down or restrict the flow of data (such as data localization measures) causes friction within the system. This friction may increase barriers to market entry, access to said tools, and undermine businesses' ability to expand to overseas markets. Further, limitations to data flows have a much wider impact to an economy through reduced consumer choice and access, and repercussions on broader economic growth and innovation.

There is of course a need for economies to localize some forms of data, such as data in which the compromise would be expected to directly and materially threaten the internal stability of an economy, or cause demonstrable long-term damage to the economy, result in immediate and exceptionally grave damage to the effectiveness of defense and security, intelligence operations, or crime prevention.

However, issues arise when data localization measures are applied to *all forms of data* (i.e., mandating that data generated within a jurisdiction, or by citizens and entities within that jurisdiction, is collected, stored, and processed exclusively within the jurisdiction itself) as a seemingly straightforward regulatory solution assuming that privacy and/or security is enhanced by defining *where* data is located.

Further, the development and use of data-driven technologies is highly dependent on large quantities of data to function. For example, deep learning-based models of AI development rely on principles of self-teaching, which train algorithms to fulfill specific functions using enormous datasets to pinpoint ideal approaches. Many of the applications of AI in use today within commonly used functions, such as adaptive search, remain continuously dependent on the input of large quantities

of data. In addition, additive manufacturing involves the reproduction of a digitally created object in a physical medium, such as plastic, metal or even living tissue.

This may bring about a drastic shortening of supply chains across many industries, including electronics, precision engineering and medicine. The viability of additive manufacturing as a process is dependent on the ability of businesses to trade and transfer in Computer-Aided Design (CAD) schematics and similar design documents in ways that ensure the integrity of Intellectual Property (IP) rights and other principles of proprietary data management.

What are some considerations and challenges?

Regulators need to strike a delicate balance between regimes which adequately address data transfer issues and promoting a business-friendly environment which still enables the flow of data. Different challenges emerge across different uses of data within emergent technologies.

Cloud computing leverages infrastructure built by dedicated service providers to provide organizations with access to powerful applications and capabilities which are often designed to be scalable according to the needs of individual customers. These services have become a cornerstone of successful digitalization efforts by governments and businesses and play a role in enabling access to advanced functions such as AI. However, cloud computing is strongly dependent on the need for uninhibited, frictionless data flows across borders. Regulatory regimes which prevent or otherwise inhibit access to data located outside domestic boundaries run the risk of limiting access to cloud computing—potentially handicapping business competitiveness and limiting the effectiveness of digitalization.

A lack of access to data is a fundamental bottleneck to data-driven technologies, including the development of AI systems—and this has implications in the context of access to data across borders as well. The use of datasets which are insufficiently robust often results in models with impaired functionality and thus limited marketability. The ability to access data across borders is thus a necessity for businesses which might operate in jurisdictions too small to generate the critical mass of data necessary to create a fully functional deep learning-based AI model. For governments and academia, ongoing research on emergent models of AI will also depend on secure access to datasets of not just adequate size, but also increasingly stringent standards of quality and traceability.

The viability of additive manufacturing as a process is dependent on the ability of businesses to trade and transfer in Computer-Aided Design (CAD) schematics and similar design documents in ways that ensure the integrity of Intellectual Property (IP) rights and other principles of proprietary data management. A given jurisdiction's failure to implement a sufficiently cohesive and enforceable framework of regulatory protections for cross-border data transfers would inherently reduce the competitiveness of its manufacturing industries, as businesses seeking to develop additive manufacturing capabilities may find themselves unable to secure access to CAD schematics and other data necessary to facilitate their work, if they are held by businesses overseas. This may in turn hamper the progression of outsourcing-oriented manufacturing industries up global value chains, as

contracts involving higher-value products may be deemed too valuable to risk, if regulatory regimes are inadequate to the task of protecting them.

Examples of emerging practices

- Language pertaining to the transfer of information across borders has become commonplace within international trade agreements such as the **Comprehensive Trans-Paciifc Partnership (CPTPP)** and **Regional Comprehensive Economic Partnership (RCEP)**. Within the CPTPP, Article 14.11 addresses the Cross-Border Transfer of Information by Electronic Means and calls for all signatory parties to allow for relevant electronic information transfers for the conduct of business by entities covered by the agreement.[168] Article 14.13 meanwhile addresses restrictions associated with requiring the use and location of computing facilities within a signatory economy's territory. Similar language to Articles 14.11 and 14.13 of the CPTPP exists within Article 12.15 and 12.14 of the RCEP, respectively.[169] Direct reference to Articles 14.11 and 14.13 of the CPTPP is further enshrined within Articles 4.4 and 4.3 of the **Digital Economy Partnership Agreement (DEPA)** signed by Singapore, Chile and New Zealand.[170]
- There is a growing demand for data for digital products and services in Viet Nam. However, much of the data processed in this context is in English—limiting its utility in the context of developing products and services focusing on Natural Language Processing (NLP) in Viet Nam, as this would require a large amount of data on Vietnamese.[171] Vietnamese telecoms group Viettel has launched the **Viettel Data Mining Platform** with the aim of improving access to Vietnamese data for government and businesses.[172] The Viettel Data Mining Platform can also provide real-time information or reports based on the data it holds and centralizes, reducing the need to gather information from different sources.
- Singapore hosts a diverse range of visitors, who often display distinct habits and cultural preferences. Seeking to comprehend and adapt to these differences, the Singapore Tourism Board (STB) commissioned the creation of the **Singapore Tourism Analytics Network (Stan).** Stan is a data analytics platform which allows hotels and tour agencies to access tourist data aggregated by the STB and its industry partners.[173] This data includes information related to tourist spending patterns, travel modes and patterns, lengths of stay in hotels, and the duration of activities participated in.
- The Indonesian government has struggled to track tourism data on sites where border gates did not have 24/7 immigration services or where border surveys were too costly to implement due to the remoteness of sites and high transportation costs. Indonesia's statistical agency Badan Pusat Statistik (BPS) has collaborated with the Ministry of Tourism

[168] Ministry of Foreign Affairs and Trade (New Zealand) (2016) Chapter 14, www.mfat.govt.nz/assets/Trade-agreements/TPP/Text-ENGLISH/14.-Electronic-Commerce-Chapter.pdf
[169] RCEP Secretariat (2020) Chapter 12, https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf
[170] Ministry of Foreign Affairs and Trade (New Zealand) (2020) DEPA Signing Text, www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Signing-Text-11-June-2020-GMT-v3.pdf
[171] VietnamNet (2020) Nền tảng "Make in Vietnam" hỗ trợ doanh nghiệp ra quyết định thông minh, https://vietnamnet.vn/vn/thong-tin-truyen-thong/nen-tang-make-in-vietnam-ho-tro-doanh-nghiep-ra-quyet-dinh-thong-minh-698468.html
[172] Nhan Dan Online (2020) First 'Made-in-Vietnam' data mining platform debuted, https://en.nhandan.com.vn/scitech/item/9411702-first-%E2%80%98made-in-vietnam%E2%80%99-data-mining-platform-debuted.html
[173] STB (2021) About Stan, https://stan.stb.gov.sg/content/stan/en/about-stan.html

and is working with telecommunications provider Telkomsel to **use Mobile Positioning Data (MPD) to track inbound, outbound, and domestic tourism data.** MPD refers to the signaling data collected by the telecommunications service provider, which is tracked by base stations regardless of caller activity. This ensures that all visitors with telecommunications devices can be passively monitored.

Key takeaways

- A delicate balance must be maintained between creating sufficiently rigorous regulatory infrastructure to support cross-border data flows and ensuring that the digital economy remains business-friendly.
- The trade and exchange of data for use within these emergent technologies is thus a significant emerging dimension of digital trade for businesses more generally as well.
- While governments and businesses in individual economies may possess significant stores of useful data, sharing data across borders may allow for the development of a more diverse range of products and services, which can more efficiently cater to much larger consumer bases.

3.1.2 Data Sovereignty

What is the issue?

Data sovereignty is premised on the idea that economies within which data is collected, held, or processed, are able to use their laws and regulatory structures to access or otherwise affect the data in question. The concept often addresses the ability of an economy to enact sovereign rights (i.e., control or ownership) over data assets which are in turn understood to be resources intrinsic and inalienably attributable to their originating jurisdictions—howsoever that may be defined.

Why is it an issue?

Various economies are taking different stances on both the issue of data sovereignty and the underlying principle. The rise in adoption and application of the concept is largely playing out along two tracks: i) economies perceive security vulnerabilities resulting from the greater exposure of domestically produced data to data owners or processors in other jurisdictions; and ii) there is an elevated understanding of the economic potential associated with *control* over data resources.

However, this has not been accompanied by a consensus regarding fundamental definitions of what data sovereignty actually means—or a concerted consideration of the concept's broader implications. Complications with regards to jurisdiction arise when considering whether economies have authority over data that is generated outside their territorial boundaries, but which may be stored within them. Further issues emerge in the context of economies which might choose to exert sovereignty over data that is attributable to their citizens, or even multinational corporations headquartered within their territories. An over-arching factor complicating all these discussions even further is the amorphousness of the concept of data sovereignty itself—a factor underwritten by the multiplicity of divergent definitions under consideration across different jurisdictions.

As more economies and multilateral organizations gravitate towards data sovereignty, achieving consensus on the concept's definition, and collectively addressing the implications associated with it

will be key to avoiding ambiguities which may hamper the development of data use cases and inhibit transparency and interoperability.

What are some considerations and challenges?

A principle of data sovereignty asserts that data held within an economy is subject to that economy's laws and regulatory structures. This imposes an additional layer of regulatory obligation onto data owners and processors, beyond those imposed in the context of corporate data governance. This risks scaling up regulatory costs associated with compliance, as burdens related to ensuring the traceability of data would naturally increase. Such obligations may furthermore multiply exponentially when considering the need to apply sovereignty to individual data assets, which due to the proliferation of cloud computing and its associated principles of data protection and redundancy, may be copied to multiple data centers across the world. Establishing which data sovereignty or sovereignties are applicable in such scenarios, and complying with relevant obligations, may add significant complexity to cross-border data flows.

A further challenge arising from applying data sovereignty is the prospect of multi-jurisdictional claims on individual data assets. Imposing sovereignty on a single data asset may result multiple claimants, for example:

- Data producing economies in which data subjects are situated;
- Data holding economies in which data centers are located; and
- Data processing economies in which corporations which modify or transform data are headquartered.

There is currently a lack of consensus and clarity on which of these entities would have the strongest claim, or if all claims would need to be honored concurrently. Firstly, data owners and process face increased uncertainty due to the lack of clear and understood boundaries on regulatory obligations (i.e., if/when data sovereignty effectively puts in place an arbitrary level of control over data). Secondly, should each of these claimants impose differing data governance obligations, data owners or stewards would be forced to implement prohibitively exhaustive and potentially even contradictory governance frameworks. This would also have notable implications on the processing and transformation of data, and may inhibit the development of data-based products and services.

As noted, significant uncertainty regarding data sovereignty is also attributable to the existence of multiple divergent definitions of the concept:

- The EU utilizes the term data sovereignty in the context of seeking to vouchsafe the rights of individual European citizens to control and profit from their data.[174] Individual European citizens are thus envisioned as data sovereigns unto themselves, with the EU guaranteeing those rights—especially in the context of cloud computing-based applications where data

[174] EIT Digital (2020) European digital infrastructure and data sovereignty, https://eit.europa.eu/news-events/news/new-report-european-digital-infrastructure-and-data-sovereignty

can be transferred across borders. Data sovereignty is notably used in conjunction with digital or technological sovereignty to describe efforts to develop resilient European technological frameworks which would reduce dependence on service providers in other jurisdictions.[175]

- China primarily focuses on ensuring that the judicial sovereignty and data security of third-party economies is maintained by all companies operating within those economies, regardless of their economies of origin.[176] Data sovereignty is further used alongside Cyber or Internet Sovereignty, which is viewed as a basis for securing the development of its digital economy.[177]
- The United States CLOUD Act of 2018 amends the Stored Communications Act of 1986 following the Microsoft Case vs United States case. The Act speeds access to electronic

[175] EUR-Lex (2021) Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee Of The Regions 2030 Digital Compass: the European way for the Digital Decade, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

[176] Global Times of China (2020) China launches global data security initiative, respects data sovereignty, www.globaltimes.cn/content/1200228.shtml#:~:text=China%20launches%20global%20data%20security%20initiative%2C%20respects%20data%20sovereignty,-By%20Wang%20Wenwen&text=China%20also%20called%20on%20states,overseas%20in%20their%20own%20territory

[177] Global Times of China (2019) US must respect China's digital sovereignty, www.globaltimes.cn/content/1143392.shtml

> information held by U.S.-based global providers in law enforcement cases. It authorizes bilateral agreements between the United States and trusted foreign partners while at the same time ensuring a high level of protection of those citizens' rights.[178]

Divergent and unclear views of data sovereignty further threaten to complicate discussions regarding data access on issues such as law enforcement. Governments in some economies may assert sovereign rights to data held by private corporations which operate on their territory, or process data produced by their citizens.

This adds an additional dimension to existing procedures and agreements which govern the rights of law enforcement authorities to access privately held data and might function to undermine checks and balances that would otherwise have provided data owners with clarity regarding their responsibilities and avenues for recourse, in cases where law enforcement agencies issued requests for access to data. Uncertainty with regards to the limits of data sovereignty—and jurisdictional authority of more than one claimant—may further incline data owners towards caution with regards to releasing data, potentially resulting in delays to enforcement.

Key takeaways

- There is no strong consensus regarding the definition and limits of data sovereignty despite the concept's growing popularity among economies and multilateral organizations.
- This lack of consensus threatens to significantly curb the development of the digital economy, due to the potential imposition of significant additional compliance obligations upon data owners and processors, beyond existing corporate data governance principles.
- A substantive challenge is the multiplicity of divergent definitions of data sovereignty, and which may individually be ill-defined in ways which may compromise accountability and substantially increase compliance costs.
- The assertion of sovereign rights to data may furthermore undermine established agreements regarding access to data by law enforcement which, in conjunction with a lack of clarity on the limits of sovereignty, also undermine law enforcement mechanisms more broadly.

[178] US Department of Justice (2021) CLOUD Act Resources, www.justice.gov/dag/cloudact

3.2 Process Enablers

3.2.1 Data Transfer Mechanisms

What is the issue?

For information to be transferred across borders securely, economies have to recognize each other's data privacy and protection regimes. Data transfer mechanisms, such as certifications and data transfer agreements, help to bridge differences in data protection and privacy laws without requiring laws to be revised. In recent years, mechanisms that seek to facilitate interoperability across data protection/privacy regimes have emerged, providing an avenue to ease compliance costs and business uncertainty, allowing innovative digital offerings to penetrate local markets, and at the same time ensuring the safe and secure flow of data.

Why is it an issue?

Agreeing on and adopting data transfer mechanisms will enable governments within regional groupings to reap the rewards brought about by increasing economic integration across their regions. These mechanisms provide guidelines helping governments and businesses to ensure that basic standards are observed with regards to the management, transfer, and use of data across all applications within the region.

Broad regional acceptance of basic tenets for the data management and transfer will furthermore promote the development of similar norms across all economies in the region, ensuring that first movers are able to share best practices with emerging economies—easing developmental divides which may exist in the context of uneven regional development.

Data transfer mechanisms can also play an important part in promoting more open mindsets towards the use and sharing of data by businesses, while also facilitating a more cohesive approach to data sharing between jurisdictions, in a regional and global context.

What are some considerations and challenges?

When regional or multilateral organizations develop certification programs, they can mitigate uncertainty with regards to otherwise divergent regulatory regimes between different member economies. For example, the APEC CBPR system provides a mechanism that enables trust and data flows amongst participants. This occurs even in the absence of governments formally recognizing that another jurisdiction has equivalent protection. Instead, APEC relies on business to use mechanisms, such as a contract, to ensure that data collected and then sent to third parties (either domestically or overseas) continue to protect the data to the requisite privacy standards.

The APEC CBPRs require independent entities who can monitor and hold businesses *accountable*. This improves ease of doing business at a regional level and allows for much greater economic

integration by adhering to a single set of requirements, and ensuring consistency of regulatory oversight and enforcement regimes across jurisdictions.

The EU's General Data Protection Regulation (GDPR), which harmonizes regulations *within* the EU, has enabled bi-lateral agreements between the European Commission and individual economies to be established based upon other economies having comparable and *adequate* data protection safeguards in place.[179] For example, the EU and Japan have agreed to enter into a mutual adequacy arrangement, formally recognizing each other's data protection laws, thereby allowing data to flow freely and safely.[180]

However, such an agreement does not come without its implementation hurdles. In order to bridge the differences between the two data protection regimes and adhere to EU's higher standards, Japan has committed to adopting additional measures. Japan will put in place safeguards to strengthen protection of sensitive data and enable individuals to exercise their right to access and rectify personal data; these will be binding on Japanese companies importing data from the EU. As part of the adequacy arrangement, Japan will also be required to establish a system to address and resolve complaints about access of European data by Japanese authorities.

At a more granular level, the development of standard contractual clauses will provide legal bases for businesses to embark on cross-border data sharing exercises more effectively, and possibly facilitate the development of industry-led cross-border data sharing initiatives. Embarking on cross-border data transfers is often intimidating because of the uncertainties involved with ensuring adequacy of protection for data—especially if the data involved is personal data—along with complying with other regulatory obligations.

The development of regional and international standard contractual clauses which establish foundational obligations including data protection measures, addresses key obstacles to cross-border data sharing. In the immediate or short term, this can manifest in the development, circulation and promotion of voluntary and non-binding model contractual clauses based on international best practices. The institutional assurance such mechanisms engender could encourage smaller regional or domestic businesses to reach out to form data sharing partnerships in the region and beyond.

Adopting data transfer mechanisms at the regional level which do not take reference from wider global and industry trends may result in regional mechanisms and transfer regimes being incompatible with international approaches and thus render them ineffectual. International

[179] As per Regulation (EU) 2016/679, the European Commission can assess whether an economy outside the European Union has adequate data protection, either through their domestic regulations or by the international commitments it has entered into, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[180] European Commission, http://europa.eu/rapid/press-release_IP-18-4501_en.htm

standards of data management and interchange should be considered to ensure that regional frameworks are aligned and interoperable with international norms.

The adoption of existing standards on information security such as ISO/IEC27001, ISO/IEC27002, ISO/IEC38505-1 and ISO/IEC 277001 should thus be encouraged within regional frameworks.[181] Alongside this, however, governments should collaborate regionally to contribute substantively to international discussions on data management, such as those being undertaken under ISO/IEC JTC 1/SC 32 on Data Management and Interchange.[182] Doing so would ensure that standards-setting exercises are inflected by an understanding of specific needs unique to regional contexts, while ensuring that local actors are well-informed about international standards when opportunities arise to develop domestic standards.

Participation within these discussions by individual members of regional groupings also represents an opportunity for norms adopted within the regional grouping to attain international recognition and become normalized beyond the regional context, which contributes to overall regional competitiveness.

Examples of emerging practices

- **APEC CBPR system** is a voluntary system that takes a flexible approach towards standardizing data protection controls and enabling cross-border flows. For example, Singapore, a participating economy in the APEC CBPR system, recognizes CBPR-certified overseas recipients of personal data as having comparable protection to organizations legally bound by the domestic data protection law, exempting CBPR-certified organizations from additional steps to demonstrate compliance with the domestic law.[183]
- **Association of Southeast Asian Nations (ASEAN)** recently introduced the ASEAN Data Management Framework (DMF) and Model Contractual Clauses (MCCs) for Cross-Border Data Flows.[184] The DMF provides a guide for businesses to introduce data management systems, while the MCCs facilitate personal data transfers across businesses in the region by providing optimized contractual frameworks for businesses to emulate or adopt, to cost-effectively reduce legal liability. Development on the DMF and MCCs was furthermore led by Singapore, reflecting the capacity for more advanced economies in regional groupings to help to bridge developmental divides by sharing information and building capacity. In this way, ASEAN is able to demonstrate thought leadership on important regulatory issues,

[181] International Organization for Standardization (2013), ISO/IEC27001, www.iso.org/isoiec-27001-information-security.html; International Organization for Standardization (2013), ISO/IEC27002, www.iso.org/standard/54533.html; International Organization for Standardization (2017), ISO/IEC38505-1, www.iso.org/standard/56639.html; International Organization for Standardization (2019), www.iso.org/standard/71670.html
[182] International Organization for Standardization (2021), ISO/IEC JTC 1/SC 32, www.iso.org/committee/45342.html
[183] Personal Data Protection Commission Singapore (2020) Singapore Now Recognises APEC CBPR and PRP Certifications Under PDPA, www.pdpc.gov.sg/news-and-events/announcements/2020/06/singapore-now-recognises-apec-cbpr-and-prp-certifications-under-pdpa
[184] Singapore Personal Data Protection Commission (2021), ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows, www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows

ensuring that developing member-states have cohesive and effective frameworks to shape their own regulatory regimes.

- **Japan's** AI Data Consortium (AIDC) launched the AIDC Data Cloud, which is a data trading platform which connects data providers with data users, and acts as an intermediary to manage the data to ensure quality. [185] The AIDC Data Cloud platform seeks to assist data users in overcoming high regulatory barriers in accessing and transforming data for use in AI applications. A core focus of the platform is ensuring that concerns about legal liability do not dissuade potential data users from accessing and using data. The AIDC Data Cloud thus provides model contractual terms in a customizable smart contract platform designed to make purchasing and sharing data as efficient and transparent as possible for data users. This limits legal liability for data users without adding to costs that might otherwise be incurred in independently formulating contracts.
- **New Zealand** introduced Privacy Principle 12 in its Privacy Act 2020, enabling businesses and other organizations to disclose personal information to foreign entities which are subject to comparable protections on private data.[186] Under Privacy Principle 12, businesses are required to have reasonable grounds to believe that data is being disclosed to an overseas partner that provides adequate protections to those offered by the New Zealand Privacy Act 2020. Any disclosures to entities which do not provide such assurances—including in the context of using cloud services—must receive the express consent of data originators. Privacy Principle 12 notably differs from the EU GDPR's adequacy decisions in that final effective authority on disclosure decisions lies with disclosing organizations as opposed to government itself.

Key takeaways

- Data transfer mechanisms can reduce friction in cross-border data flows by smoothing over differences in data management regimes across different jurisdictions.
- There are diverse approaches to developing data transfer mechanisms, ranging from certification regimes and adequacy considerations to more granular mechanisms such as model and standard contractual clauses.
- Data transfer mechanisms should consider international standards and best practices to ensure that adopted approaches are aligned with global approaches and facilitate interoperability.
- Businesses stand to benefit most from the development of data transfer mechanisms due to the removal of uncertainties regarding legal and compliance obligations. A lack of data transfer mechanisms can limit businesses seeking to do business with regional or international partners.
- The development of data transfer mechanisms can be particularly beneficial for regional organizations with members which are at different stages of their development with regards to data management regulations.

---

[185] Nikkei (2021), AIデータ活用コンソーシアム、AIに対応したデータ取引サービス「AIDC Data Cloud」を発表, www.nikkei.com/article/DGXLRSP604957_Q1A210C2000000/

[186] Office of the Privacy Commissioner (2020) Privacy Principle 12, www.privacy.org.nz/privacy-act-2020/privacy-principles/12/

3.2.2 Digital Trade Standards

What is the issue?

Standards are typically a published document setting out specifications and procedures to ensure consistent implementation of processes, technologies, and methods. [187] The use of standards, when developed properly and deployed well, can enable a high benchmark for security, safety, quality, and reliability of goods and services being delivered into a market. In turn, the *implementation* of standards increases the interoperability of the processes, technologies or methods standardized across the range of producers, suppliers, and consumers.

Digital technologies evolve at a fast pace, and are often led by industry, resulting in technical specifications hardwired into regulatory frameworks becoming outdated. In this context, the standards-setting process (as compared to the development of regulations) is able to more quickly respond to changing technological, business, and regulatory conditions due to the range of participants and levels of expertise involved in the international standards-setting process.

Standards are therefore assuming an increasingly significant role in providing economies with a more flexible and fit-for-purpose approach to the evolving digital trade environment, as well as accelerating the use of digital technologies at different stages of the supply chain, which in turn is increasing the scope, speed, and scale of trade.

Why is it an issue?

The adoption, implementation, and use of international standards is crucial, and provides numerous benefits for APEC member economies, including:

- **Interoperability** in digital systems for transparency, simplicity, and compliance;
- **Mutual compatibility** in products, components, and services, especially where digital developments have created new products, components or services, or introduced elements of risk;
- **Flexibility** and promptness in responding to new challenges or changes in such processes that will inevitably occur as digital economy and digital trade frameworks continue to adapt and change; and
- **Consistency** in the quality of goods or services, with appropriate safety and security safeguards.

[187] International Organization for Standardization (2004) Standardization and related activities – General vocabulary, https://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/8389141/ISO_IEC_Guide_2_2004_%28Multilingual%29_-_Standardization_and_related_activities_--_General_vocabulary.pdf?nodeid=8387841&vernum=-2

Standards bring benefits to businesses in terms of substantially larger (potentially global) markets, reduced costs, standardized processes, and compliance, as well as enhanced productivity. By making trade easier and more efficient, they bring benefits to the overall economy.[188]

International standards facilitate interconnectivity and interoperability by setting out specifications and procedures to ensure consistent implementation of processes, technologies, and methods. Interconnectivity of networks allows traffic to travel across and between networks. This will for instance, enable economies of scale as the fixed costs of infrastructure rollout are spread across a greater level of output bringing about a fall in unit costs.

Interoperability of systems, software and operating platforms means that traffic can run effectively across different types of networks (e.g., from telecoms to banking to logistics to educational to health networks and so on). This too enables economies of scale, as fixed costs are spread across a wider range of output of different goods and services. Scale is associated with reach—the ability of a system to serve the greatest number of users. Enabling access by those previously unable to benefit from new systems.

International standards play a key role in aligning rules and processes across borders to minimize both incompatibilities among domestic approaches as well as regulatory uncertainty. With the development of new industries such as components for autonomous vehicles or use of new technologies such as blockchain for existing industries—failure to participate in international standards and processes can inevitably lead to product or service incompatibility, causing market inefficiencies.

What are some considerations and challenges?

The encompassed activities considered to be within the scope of digital trade is only expected to increase as new technologies such as the IoT, AI, 5G mobile communications, and developments such as blockchain gain traction, and both economies and communities become more interconnected.

However, what is often less well recognized are the requirements for commodities and traditional goods such as white goods (or traditional services such as bookkeeping) to be digitally standardized for the global trade in data to be enabled. For IoT and 5G to work at scale—fridges, toasters, hair irons, ice machines, and air conditioners need to be standardized in line with the communications protocols. This is what is currently playing out for example in autonomous vehicles and smart homes.

In recent years it has been the standards in payments, in electricity (for data center power delivery), in storage, and in containers, which have been important in establishing digital trade agreements.

---

[188] BSI Group (2015) The economic contribution of standards to the UK economy, www.bsigroup.com/LocalFiles/en-GB/standards/BSI-The-Economic-Contribution-of-Standards-to-the-UK-Economy-UK-EN.pdf

Much of what needs to be focused upon as *emerging digital trade standards* will therefore need a wide canvas and an understanding of digital development as a first step.

APEC economies should be encouraged to actively contribute to the development of international standards. However, it needs to be recognized that the standards-setting processes have moved beyond the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and International Telecommunication Union (ITU) processes—with industry bodies leading the charge, with EMVCo Technical Specifications for QR codes[189] being the standout example, along with the FIDO Universal Authentication Framework[190] for digital identities, APIs for open banking, and even AI ethics.

Examples of emerging practices

- **Security:** The ISO/IEC 27000 family of standards are often referenced and have become the foundational security standards that enable robust and consistent data protection and privacy measures, which increase community trust in all types of digital initiatives, driving adoption and use. Commonly adopted standards for information security include ISO/IEC27001, ISO/IEC27002, ISO/IEC38505-1 and ISO/IEC 277001.[191]
- **Data exchange:** The ISO technical committee ISO/TC 204 on Intelligent Transport Systems, has been working closely with other ISO technical committees, OASIS, IATA, IEC, CEN, the UN/CEFACT and the WCO to develop collaborative and interoperable standards.[192] The technical specification ISO/TS 24533 was developed to allow electronic data sharing through a many-to-many relationships between supply chain partners. The UN/EDIFACT (the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport) is a leading global standard for EDI accounting and is used by 90% of all carriers/agents, 95% of all terminal operators, 80% of the world's port authorities, 97% of customs administrations, and 40% of road/barge/rail planning.[193]

Key takeaways

- While digital economies and the flow of data grows, approaches to implementing new digital technologies are becoming more complex and, in some cases, divergent. New standards are being created by domestic standards bodies in order to put in place safeguards for government agencies, businesses and consumers that use digital technologies. While there are benefits to setting standards and there may be valid regulatory objectives, there is a risk that domestic efforts may create barriers that impede trade. It could lead to disparate

[189] EMV were originally the companies of Europay, Mastercard, and Visa, who created the standard for cards and chip payments. Today EMV is known as EMVCo, a consortium of financial companies, which develops standards in mobile, Payment Tokenisation, 3-D Secure, QR Code, Secure Remote Commerce. www.emvco.com/about/overview/
[190] FIDO Alliance, https://fidoalliance.org
[191] International Organization for Standardization (2013), ISO/IEC27001, www.iso.org/isoiec-27001-information-security.html; International Organization for Standardization (2013), ISO/IEC27002, www.iso.org/standard/54533.html; International Organization for Standardization (2017), ISO/IEC38505-1, www.iso.org/standard/56639.html; International Organization for Standardization (2019), www.iso.org/standard/71670.html
[192] ISO (2017) Why Intelligent Supply Chains Will Rule The World, www.iso.org/news/ref2214.html
[193] UNECE (2018) Report on the use of United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Standards, www.unece.org/fileadmin/DAM/cefact/cf_plenary/2018_plenary/ECE_TRADE_C_CEFACT_2018_INF.2.pdf

technologies and platforms that are unconnected and unable to facilitate a seamless flow of cross-border trade.

- APEC economies should be actively involved in contributing to the development of international standards. However, this needs to go beyond participating in standards-setting processes to *driving* the development of international standards in order to forward APEC economic interests. This should involve re-positioning standards as an opportunity to drive innovation, rather than an operational back-office initiative.
- As such, APEC needs to and should create a lighthouse effect on key digital trade standards in priority areas such as finance, security, infrastructure, cloud computing, and 5G.

3.3 Emerging Issues

3.3.1 Regulatory Fragmentation

What is the issue?

There are a variety (and rapidly increasing number) of different *types* of regulations relevant to the digital economy (e.g., data protection and privacy, cybersecurity, online consumer protection, and various sectoral regulatory applications, as well as emerging data sharing and AI requirements), with many economies at vastly different stages of creating, implementing, or enforcing these regulations.

Domestic legal and regulatory drivers are resulting in quite different applications of similar issues across jurisdictions. The result is an increasingly complex—and complicated—landscape of regional regulatory compliance requirements with many digital regulatory requirements being incompatible across economies—i.e., regulatory regimes not 'talking' to each other, or being interoperable.

Why is it an issue?

This regulatory fragmentation creates barriers not only for cross-border business—increasing compliance costs—but also generates a 'drag' on the potential economies of scale and scope available to an economy (and the businesses within) resulting in missed opportunities to trade.

The extent of regulatory fragmentation is very likely to increase due to ongoing pressures to speed up economic recovery from COVID-19 (with economies focusing on domestic markets over cross-border trade), and inconsistent implementation of international standards.

What are some considerations and challenges?

Seizing the opportunity presented by digital trade, and realizing its potential for economic growth of APEC, will depend on the development and implementation of harmonized digital trade rules. Trade rules help remove a host of barriers impeding trade such as cross-border data flow restrictions, localization requirements, tariffs and quotas on ICT equipment, domestic and local standards that deviate from international standards, and lack of access to effective dispute resolution mechanisms. They also promote cooperation among economies by encouraging individual economies to move away from putting in place rules that are protectionist in nature, and hinder the growth of digital trade.

Given the central role of data flows, recent digital trade agreements such as Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[194] Singapore-Australia Digital Economy

[194] Government of Canada (2021) CPTPP, www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/toc-tdm.aspx?lang=eng

Agreement (SADEA),[195] DEPA,[196] and the Regional Comprehensive Economic Partnership Agreement (RCEP),[197] all include commitments to support cross-border transfers, and limit localization mandates, to facilitate digital trade in the region and support trust and confidence in the digital environment:

- **Promotion of cross-border data flows:** Provisions aim to ensure that businesses can utilize data and capitalize on digital opportunities across the world. The agreements contain commitments that the members will promote the free flow of information across borders, while preserving an economy's right to protect its data for legitimate public policy and security objectives. They also do not affect an economy's right to establish its own domestic policies and regulatory frameworks, or weaken existing frameworks.
- **Elimination of data localization measures**: Provisions relating to data localization include commitments to prevent members from requiring computing facilities to be located in their territory. The provisions are aimed at reducing costs for businesses, who may be forced to build data storage centers and use local facilities within each economy that they trade with. The commitments are also exemptions for achieving legitimate public policy objectives.

The digital trade rules pertaining to data flows agreed upon by members in these trade agreements hold immense potential. They allow economies to come together and in theory exercise a high degree of influence over rules governing data flows, and consequently global trade. For instance, RCEP as an economic bloc represents 30%[198] of the world's GDP, and CPTPP accounts for a substantial 13.5%[199] of the world's GDP. Therefore, these agreements may also serve to prevent non-member economies from imposing restrictions on data flows.

Data-related policies across the APEC region, as well as other parts of the world have become *more* inward looking, prioritizing issues of data sovereignty and the retention of data within borders.[200] Commitments made in digital trade agreements to facilitate cross-border transfers provide a path forward. Members can build on these provisions and further reduce restrictions, such as on sectoral data and data storage locations. Sectors such as finance for instance have traditionally seen the most stringent restrictions. The United States-Mexico-Canada Agreement (USMCA) has already begun to address this by including explicit provisions for access to financial information for oversight.

---

[195] DFAT (2021) Singapore-Australia Digital Trade Agreement (SADEA), www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement
[196] MTI (2020) Digital Economy Partnership Agreement (DEPA), www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement
[197] DFAT (2020) Regional Comprehensive Economic Partnership (RCEP), www.dfat.gov.au/trade/agreements/not-yet-in-force/rcep
[198] World Economic Forum (2021) What is RCEP, the world's biggest trade deal? www.weforum.org/agenda/2021/05/rcep-world-biggest-trade-deal
[199] Atlantic Council (2020) Global and Regional Trade Systems, www.atlanticcouncil.org/in-depth-research-reports/issue-brief/global-and-regional-trade-systems
[200] ITIF (2021) How barriers to cross-border data flows are spreading globally, what they cost, and how to address them, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

Examples of emerging practices

Provisions in digital trade agreements are also key to bringing more convergence in approaches to data flows. Increasingly, privacy laws have a high degree of variance in the requirements for cross-border transfers of personal data, even as digital consumption has skyrocketed through the pandemic. This heterogeneity of requirements adds to regulatory complexity and uncertainty, resulting in less transparency, as well as less clarity on rules.

While these provisions may not be able to address regulatory convergence directly, the cooperative, non-binding nature of these trade rules can be key to developing common data standards and architectures, that enable interoperability and information exchange.[201]

- SADEA provisions establish that both parties will consider the principles and guidelines of relevant international bodies such as APEC Cross-Border Privacy Rules (CBPR)[202] and OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data[203] and recognize the CBPR as a valid mechanism to facilitate cross-border data while protecting personal information.

Key takeaways

- Domestic digital economy developments have been growing exponentially, but in parallel domestic digital regulations have been growing equally fast.
- This regulation paradox has resulted in ever more constraints being placed on digital trade, and an increasingly fragmented and complex international environment to navigate.
- Increasingly, digital trade standards and digital trade agreements are bridging this gap and enabling systems and processes to interoperate and talk to each other.

[201] World Bank (2021) Crossing Borders, https://wdr2021.worldbank.org/stories/crossing-borders
[202] APEC Cross-Border Privacy Rules System, www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System
[203] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

3.3.2 Digital Regulatory Arbitrage

What is the issue?

Regulatory arbitrage occurs where different jurisdictions create different sets of laws and regulations, and persons or corporate entities that operate across borders have the opportunity to take advantage of whichever offers the greater benefits, for example in taxation, in labor laws, in health and safety standards, or in consumer protection.

The global Internet has greatly increased the ease and speed at which persons and corporate entities using a digital presence can exploit these opportunities for arbitrage. This is also a major driver behind global value chains (GVCs). The complexity of these arrangements requires a veritable army of accountants and lawyers on both sides of the fence to calculate where the benefits lie—or are escaping to. While the resources of leading economies can hope to manage these "arm's length principle" (ALP),[204] developing economies cannot.

Digital regulatory arbitrage has been further compounded by various economies seeking to establish the global regulatory precedence of *their* requirements through extraterritorial application. This in turn has led multinational companies and digital platforms to choose the most onerous set of requirements for compliance (and competition) purposes, and governments are now trying to game this system by prescriptively framing new rules to specifically around certain companies (e.g., Google, Facebook, Alibaba) rather than desired economic and social outcomes.

Why is it an issue?

At a business-to-business level, regulatory arbitrage is frequently used by these global companies to move their assets and their sale invoices around to avoid local regulations and taxes. This is avoidance, exploiting different regulatory regimes, but not illegal evasion. Different regulatory jurisdictions that are not in close harmony, which use different standards, and which have no treaties or arrangements to establish equivalence between each other, provide the gaps in the global trading system for such arbitrage.

Additionally, when the sale of goods and services are invoiced in one economy, but the purchaser resides in another, regulators need to establish a criterion for assessing which geographical market is involved. These issues are currently matters of discussion within the OECD to achieve a consistency and a certainty globally.

For developing economies especially, there is often a trade-off between the need to attract foreign investment and the need to raise revenue through taxation. To avoid double taxation, Tax Treaties

[204] UNCTAD (2018) International tax, regulatory arbitrage and the growth of transnational corporations, https://unctad.org/system/files/official-document/diaeia2018d5a3_en.pdf

(otherwise known as International Investment Agreements or IIAs) are one vehicle to make an economy appear attractive to foreign capital in the expectation that there will be a trade-off between the arrival of investment at low rates of taxation, perhaps with tax holidays and other benefits such as land grants attached, and local job creation and the transfer of technology and knowhow.

The Internet has made regulatory arbitrage easier to manage because global companies (alternatively referred to as international, multinational, or transnational companies) are able to create multiple subsidiaries which can be registered digitally in different jurisdictions. This is a major driver behind global value chains (GVC). These companies can then use transfer pricing to shift taxable revenues from one jurisdiction to another.

The complexity of these arrangements (recognized by the OECD as Transfer Pricing Guidelines or TPGs) requires a veritable army of tax accountants and lawyers on both sides of the fence to calculate what might be a fair and reasonable tax to pay in any single jurisdiction, and while the resources of leading economies can hope to manage these "arm's length principle" (ALP)[205] poorer economies cannot. Digital trade has magnified these issues, and they are regularly the subject of debate and negotiations between trading partners and in fora such as APEC, the OECD and others.

What are some considerations and challenges?

It is not just tax revenues from global companies that economies stand to lose through regulatory arbitrage. Poorer economies are not in a strong position to insist upon technology transfer actually happening. They can easily lose foreign exchange and currency control. The rise of digital companies means that goods and services can be paid for online using credit cards, Internet banking transfers, or from accounts held overseas. This can mean, for example, a citizen or an organization has registered a bank account overseas and is channeling funds overseas and avoiding local Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) regulations. Where such payments are made in a cryptocurrency such as Bitcoin tracking ownership and tracing payments becomes extremely difficult.

Examples of emerging practices

Broadly, there are two approaches economies can take towards digital regulatory arbitrage, and a combination of them is the most practical way. The first is to seek harmony between very different laws, regulations and standards in different economies. Global and regional membership organizations such as OECD, the G20, and APEC, spend much time and effort on this approach. This is ideal, but often difficult to achieve requiring very lengthy negotiations involving local vested interests, it takes time to implement and if implementation is patchy, it offers further arbitrage

[205] UNCTAD (2018) International tax, regulatory arbitrage and the growth of transnational corporations, https://unctad.org/system/files/official-document/diaeia2018d5a3_en.pdf

opportunities. In the meantime, due to the speed at which new digital technologies and Internet-based business models develop the revised laws can be outdated very quickly.

The second is what's called the 'Conflict of Laws' approach. To cite one authority, it is "a body of law that determines what law should apply where more than one sovereign can arguably lay claim to exercise sovereignty over an issue ... a body of law that addresses a question that has been largely ignored in global financial regulatory debates—the question of the scope (as opposed to the content) of national, international, and non-state regulation: how far does each regulatory authority extend, and what should be done when these overlap?"[206]

Key takeaways

- Leading economies can afford well-resourced tax offices and have high bargaining power in treaties and global negotiations, including *de facto* extra-territorial reach whereas poorer economies for the most part need to rely upon equitable outcomes from bodies such as the OECD and international and regional treaties which are trying to harmonize.
- A Conflict of Laws approach is pragmatic and often achievable, possibly on a bi-lateral basis, in the short-term.
- Global digital companies employ far more tax lawyers than are available to developing economies, so the real power of decision-making lies in the regulation of market access, and that power is proportional to the growth of the local economy which implies pro-growth local policies.

[206] Cornel International Law Journal (2014) Managing regulatory arbitrage: a conflict of laws approach, www.lawschool.cornell.edu/research/ILJ/upload/Riles-final.pdf