Organisation for Economic Co-operation and Development

DSTI/CDEP(2022)11/FINAL

Unclassified

English - Or. English

15 November 2022

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Digital enablers of the global economy

Background paper for the CDEP Ministerial meeting

JT03507754

Foreword

This paper discusses three underlying digital enablers of the economy – online platforms, cross-border data flows and digital security – and the challenges and opportunities they pose for policy makers. Given that these issues are international in nature, the report notes the importance of a global policy response.

This paper provides background to support discussions on Theme 1: Digital Enablers of the Global Economy of the Ministerial meeting of the Committee on Digital Economy Policy, taking place on 14-15 December 2022 in Gran Canaria, Spain. It informs the sessions on “Shaping policies for online platforms”, “Fostering trust in cross-border data flows” and “Strengthening the foundations for digital security across products and services” of the Ministerial meeting.

This paper was written by Angela Attrey, Thyme Burdon, Francesca Casalini, Simon Lange and Peter Stephens, under the supervision of Audrey Plonk, Head of the OECD Digital Economy Policy Division. It benefited from the input of Gallia Daor, and Angela Gosmann, Sebastian Ordelheide and Misha Pinkhasov provided editorial support. The Ministerial meeting and related work were generously supported by the Government of Spain.

This report was approved and declassified by written procedure by the Committee on Digital Economy Policy on 26 October 2022 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on iLibrary as:

OECD (2022), "Digital enablers of the global economy: Background paper for the CDEP Ministerial meeting", *OECD Digital Economy Papers,* No. 337, OECD Publishing, Paris, https://doi.org/10.1787/f0a7baaf-en.

Table of contents

FIGURES

Executive summary

An increasing share of global economic activity is powered by digital technologies. While these and the new business models they enable bring substantial benefits, the fundamental changes that come with them call for new policy frameworks at global scale. Despite a crowded digital landscape, three enablers stand out at the top of policy agendas:

- **Online platforms** enable transactions and interactions between multiple distinct sets of users across the world. They open markets and opportunities to consumers and businesses, including between unknown parties. However, they raise competition and consumer protection concerns. Fragmented policy and regulatory responses lead to costs and uncertainty for firms and consumers and require transnational coordination.
- **Cross-border data flows** let firms build and manage complex global supply chains, share research data and facilitate communications. However, they amplify policy concerns, causing governments to take policy and regulatory measures governing whether and how data can flow across borders. Policy makers must assess these developments and ensure that fragmentation, and lack of transparency and of regulatory clarity do not stunt economic opportunities and undermine the objectives that these regulations are meant to serve.
- **Digital security** enables confidence in and growth of the digital transformation. However, the explosive pace of digital transformation has not been accompanied by equal advances in the security of online services and connected products. End-users can rarely assess sufficient approaches to security, resulting in market failures that undermine consumer trust and put the system at risk. Many challenges facing digital security are international, as vulnerabilities and poor practices should be addressed globally to maximise impact.

The challenges associated with these enablers are best addressed through international co-operation to carefully balance national policy objectives with gains to be had from a globalised digital economy. A lack of international coordination risks creating a fragmented policy landscape that few firms will be able to navigate, and at substantial cost to consumers.

The OECD has a longstanding leadership role in digital policy, including through its international standards and policy guidance. Its expertise measuring, monitoring and assessing digital technologies and their impacts on societies is internationally recognised. The OECD also provides a model for inclusive and global multi-stakeholder dialogue. With the continued support of its members, and in dialogue with relevant international institutions and stakeholders, the OECD can support countries' ambitions for a global economy enabled by digital technologies.

1 Introduction

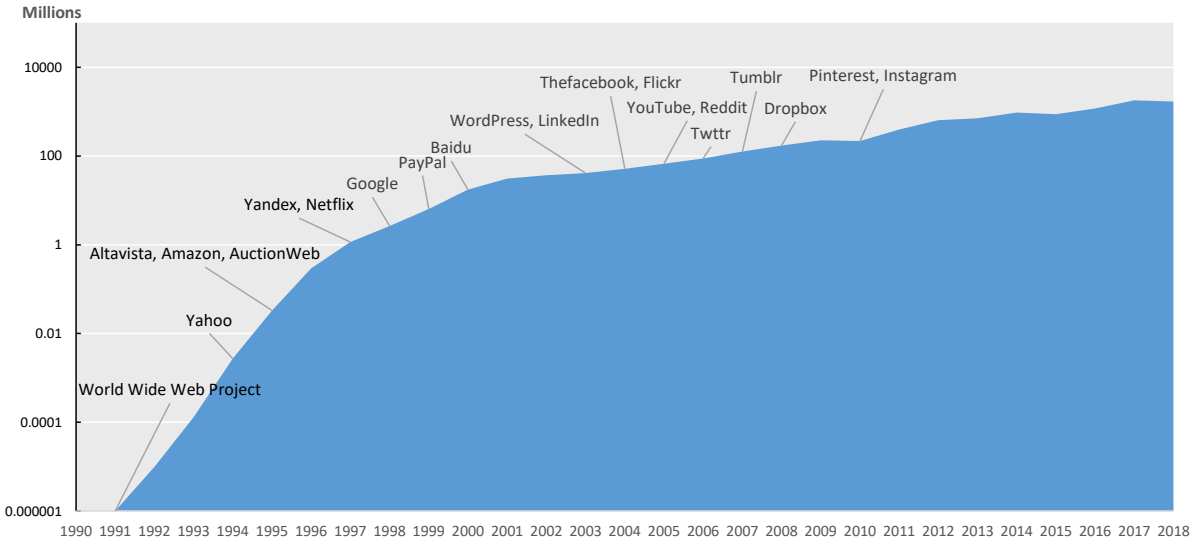
From humble beginnings, a foundation of a global economy

For early users, the World Wide Web was a strange and wondrous place full of seemingly inconsequential experimentation. The first website was published in 1991 and contained a description of what the Web was and how it could be used. By the end of 1992, only ten websites were online, which dealt in free software, random collections of information and nerdy humour. The first webcam, which started streaming at the end of 1993, monitored the level of coffee in a pot in a computer lab at the University of Cambridge.

From these humble beginnings, the number of websites grew explosively. In 1994, *Jerry and David's Guide to the World Wide Web* was launched, later re-named Yahoo. Along with web browsers like Mosaic and Netscape, released in 1993 and 1994, respectively, search engines made different parts of the Web accessible to a wider audience. Complementary innovations, like broadband and mobile technologies, helped more people go online. The Web grew from one site in 1991, to more than one million by 1997. Ten years later, there were more than 100 million (Figure 1).

Figure 1. Number of websites, 1991-2018

Millions, logarithmic scale



Note: Websites refer to unique hostnames. The number of active websites (as opposed to parked domains or similar) might be substantially lower.
Source: Netcraft (2022[1]), Web Server Survey, https://news.netcraft.com/archives/category/web-server-survey/; Gray (1996[2]), Web Growth Summary, https://www.mit.edu/people/mkgray/net/web-growth-summary.html

The Internet – the global system of interconnected computer networks – fuels innovation (OECD, 2016[3]). Behind some of the websites that appeared between 1995 and 2005 were young companies building new applications and services. Some of them, like Amazon, Baidu, Facebook, Google, Netflix and PayPal, are now household names. Competition was fierce, as witnessed by the 'browser wars' (the continuous battle for the market for Internet browsers). Platform-based businesses like Amazon, Airbnb, and Uber disrupted entire industries while traditional companies came to lean on digital technologies to optimise their processes and build intricate global supply chains.

Digital enablers of the global economy and their policy challenges

Digital technologies and services built on the Internet now underlie the global economy, facilitating new business models, connections, transactions and unprecedented access to information, regardless of geographic location. While many factors are important – from connectivity to skills – this paper examines three key digital enablers of the global economy that have risen to the top of policy agendas:

- **Online platforms.** Connecting users around the globe enables global economic activity by providing firms with access to more markets and consumers with access to more content and products. However, while the early digital ecosystem was teeming with entrepreneurial energy, there are increasing concerns that this dynamism has receded and incumbent platforms have become entrenched. Legal scholars and economists note that digital firms' market power seems to be on the rise while concerns are growing about consumer protection online.
- **Cross-border data flows.** The architecture of the Internet allows data to move seamlessly between networked devices anywhere in the world, enabling coordination of global value chains and cross-border provision of services. However governments increasingly adopt regulatory and policy measures that regulate the transfer of data across jurisdictions. Internet users increasingly feel that they, rather than coffee pots, are monitored online. This makes the protection of privacy a key concern, along with protection of intellectual property rights and other public policy objectives.
- **Digital security.** Without digital security, individuals and organisations could not confidently engage with the digital products and services that increasingly power international production and trade. As ever-larger parts of the economy come to rely on digital technologies, the stakes for digital security increase: poor security can result in emotional, financial and physical harm at an unprecedented scale. To date, the explosive pace of digital transformation has not been accompanied by a corresponding increase in security standards.

A call for global digital governance

Originally, the World Wide Web was accessible and comprehensible to very few people. Today, more than half of humanity is online in some form. As the digital transformation has progressed, most OECD countries have adopted national digital strategies (Gierten and Lesher, 2022[4]) and put in place laws, regulations and standards to protect consumers while enabling the digital transformation and ensuring it benefits all.

However, many policy challenges in this realm are international and the digital transformation needs stronger governance at global scale to allow people and businesses to take full advantage of the opportunities it affords. Policy makers must work together to find consistent approaches to governing the digital enablers of the global economy.

Box 1. Selected OECD policy research and legal instruments on digital enablers of the global economy

Online platforms

- OECD (forthcoming[5]), "Data shaping firms and markets", OECD Digital Economy Papers, OECD Publishing, Paris
- OECD (2022[6]), "The role of online marketplaces in protecting and empowering consumers: Country and business survey findings", OECD Digital Economy Papers, No. 329, OECD Publishing, Paris, https://doi.org/10.1787/9d8cc586-en
- OECD (2019[7]), An Introduction to Online Platforms and Their Role in the Digital Transformation, OECD Publishing, Paris, https://doi.org/10.1787/53e5f593-en.
- OECD (2019[8]), Unpacking E-commerce: Business Models, Trends and Policies, OECD Publishing, Paris, https://doi.org/10.1787/23561431-en
- OECD (2016[9]), Recommendation of the Council on Consumer Protection in E-Commerce

Cross-border data flows

- OECD (forthcoming[10]), "Fostering cross-border data flows with trust", OECD Digital Economy Papers, OECD Publishing, Paris
- OECD (2021[11]), Recommendation of the Council on Enhancing Access to and Sharing of Data
- OECD (2013[12]), Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (the *OECD Privacy Guidelines*)

Digital security

- OECD (forthcoming[13]), Recommendation of the Council on Digital Security Risk Management
- OECD (forthcoming[14]), Recommendation of the Council on National Digital Security Strategies
- OECD (forthcoming[15]), Recommendation of the Council on the Digital Security of Products and Services
- OECD (forthcoming[16]), Recommendation of the Council on the Treatment of Digital Security Vulnerabilities
- OECD (forthcoming[17]), Policy Framework on Digital Security
- OECD (2021[18]), "Understanding the digital security of products: An in-depth analysis", OECD Digital Economy Papers, No. 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en
- OECD (2021[19]), "Encouraging vulnerability treatment: Overview for policymakers", OECD Digital Economy Papers, No. 307, OECD Publishing, Paris, https://doi.org/10.1787/0e2615ba-en

2 Online platforms: Enabling global transactions and interactions, but disrupting policy frameworks

Online platforms are perhaps the most archetypal digital business model: a digital service that enables interactions between multiple distinct sets of users via the Internet (OECD, 2019[7]). Online platforms can open new markets and opportunities for consumers and businesses alike, enabling global transactions and interactions that would otherwise be impossible, including by providing tools that assure safe and trusted exchanges between parties unknown to each other (Burdon, 2021[20]). Platforms often provide new, high-quality products and services at low prices, or even for no monetary cost (although sometimes in exchange for data collection). Online platforms have disrupted incumbent, analogue businesses and enabled the spread of information to help consumers make informed choices, including switching between goods, services and providers (OECD, 2022[21]).

At the dawn of the World Wide Web, experimental business models rose and fell rapidly (Furman et al., 2019[22]). Since the mid-1990s, however, a handful of online platforms have become household names, attracting attention, skills, data, and revenues. While online platforms differ in size, users, and functionality (OECD, 2019[7]), policy and public interest focus on this handful of digital giants on issues from privacy to content moderation and labour-market intermediation. As this group takes the lion's share of major online markets, including e-commerce, search, online advertising and social media (OECD, 2022[21]), its effect on competition has drawn particular scrutiny.

Broader economic evidence suggests that competitive intensity in digital markets is waning. Across OECD countries, fewer firms are entering and exiting markets (OECD, 2021[23]; Bajgar et al., 2019[24]) – a phenomenon even more pronounced in digitally intensive sectors (Calvino and Criscuolo, 2019[25]). While digital start-ups attract significant equity investment and venture capital, they are increasingly acquired by larger players before they have a chance to grow and thrive (Bajgar, Criscuolo and Timmis, 2021[26]). Industries across the OECD are becoming more concentrated (Bajgar et al., 2019[24]), but especially in sectors that rely on software and data (Bajgar, Criscuolo and Timmis, 2021[26]). These trends are a concern because competition is essential for lower prices, more innovation and long-term growth and well-being (OECD, 2022[21]).

Against this backdrop, experts argue that certain digital platforms enjoy durable market power (OECD, 2022[27]; OECD, 2022[21]; OECD, 2021[28]), noting the following contributing factors:

- **Strong network effects.** As the number of users grows, the value of the product to users increases, attracting other users. This can result in a markets "tipping" into monopoly (also known as a 'winner-takes-all' effect) (OECD, 2022[21]).
- **Economies of scale.** Since the price of adding an additional user is often low, platforms can easily scale up and expand their geographic coverage without significant additional investment.
- **Data collection.** Online platforms can collect detailed data from users on all sides of a market, including consumers, advertisers and other businesses. This data can enhance product quality,

strengthen network effects, target products to different audiences and steer consumer decision-making (OECD, 2022[29]). Coupled with scale, incumbent online platforms' data advantage can pose a barrier to entry for others (OECD, 2022[27]).

- **Vertical integration, conglomerates, and cross-market linkages.** Online platforms often bundle multiple digital products, such as operating systems and devices, into a seamless, data-driven offer that may make it harder for consumers to change providers (OECD, 2022[27]). They might also leverage their dominant position in one market, such as by using their data or bundling, to enter another. Some online platforms have vertically integrated business models, which can force downstream competitors to rely on them for access to customers and could give rise to complaints of anti-competitive conduct (for example, when a platform competes downstream in the marketplace it operates) (OECD, 2021[28]).

In response, many countries have adapted traditional enforcement tools, increased the technical capacity of authorities and prioritised enforcement of competition and consumer protection laws in digital markets. In addition, often noting the structural characteristics of digital markets that can lead to concentration, many jurisdictions have moved beyond traditional tools by proposing or implementing additional regulatory initiatives that apply to a limited set of firms, usually including the largest online platforms (OECD, 2021[28]). While these regulations differ, they tend to address (OECD, 2021[28]):

- **Data-related concerns,** including obligations to grant competitors access to important datasets and implement data portability and interoperability measures.
- **Perceived 'gatekeeper' status of online platforms,** including measures related to limit self-preferencing their own goods and services and bundling.
- **Transparency and fair-business practice obligations**, including mandatory codes of conduct and requirements for the transparency of algorithms, business and advertising practices and data collection. Some proposed rules constrain how observed or inferred user-data can be retained, processed, or transferred.
- **Additional merger requirements**, including an obligation to inform regulators of all relevant mergers and acquisitions.

Although the proposed regulations share certain features and all aim to promote competition online, the measures differ substantially across jurisdictions. Otherwise, a fragmented policy and regulatory landscape for platforms carries costs for both firms and consumers, increases uncertainty and can preclude welfare-enhancing innovation (OECD, 2021[28]). Further, because the largest online platforms are global, the effects of regulations in one jurisdiction can spill over into others. A coherent global approach would enhance regulatory effectiveness and ensure that digital markets remain competitive, contestable and contribute to economic well-being.

Policy makers are also focusing on consumer-protection issues around the world. In many cases, online platforms have limited liability for illegal conduct by their users, due to their position as intermediaries connecting traders and consumers (Burdon, 2021[20]). However, a platform's ability to control its own ecosystem is one of its hallmarks because positive experiences contribute to the user retention critical for a platform's success, (OECD, 2019[7]). This is generally achieved by rules about who can join a platform and how they behave on it. Platforms can monitor user conduct to ensure that rules are followed and encourage compliance by acting against users that break them, such as by banning them.

In practice, however, despite investment in surveillance tools and processes to detect non-compliance, platforms face challenges regulating the behaviour of users. Some businesses take steps to protect consumers, but scams, unsafe and counterfeit products, and fake ratings and reviews remain in many online marketplaces (OECD, 2022[6]). This has led policy makers and competition and consumer authorities to encourage platforms towards greater self-regulation and to alternative models of government-led regulation, such as product safety pledges (OECD, 2021[30]).[1] It is also leading policy

makers to ask if platforms should face greater liability for the actions of their users, to better protect consumers.

3 Cross-border data flows: Facilitating global trade and co-operation, but raising policy concerns

The architecture of the Internet allows information to flow between and across networks and borders. Firms and consumers quickly took advantage of this to develop new business models and obtain access to global markets. Today, data flows underpin a range of international trade in goods and services. They allow firms to build and manage complex global supply chains, organisations to share data for research, and consumers to seek information about goods and services offered around the world.

While the contribution of cross-border data flows to global value-added is likely significant, it is not well understood. Value cannot be easily discerned from either trade or information and communication technology (ICT) statistics and definitive empirical evidence is still lacking. That said, ICTs have been credited with enabling the most recent wave of global integration, leading to rapid economic development in some developing countries (Baldwin, 2017[31]).

At the same time, the flow of data across borders amplifies policy concerns, based on which governments have taken measures to govern whether and how data can cross borders. Regulatory and policy rationales include (Casalini and López-Gonzalez, 2019[32]; Aaronson, 2019[33]):

- **Privacy protection.** In the case of personal data, cross-border flows raise questions about data protection and privacy, especially when domestic regulatory frameworks differ from those in receiving jurisdictions. Some governments also worry that personal data transferred abroad could be exposed to surveillance by foreign governments.
- **Security.** Governments might regulate cross-border data flows as a way to protect information they deem sensitive from a national-security perspective or to prevent harm to domestic consumers (e.g. credit card fraud, identity theft) and businesses (e.g. ransomware attacks).
- **Intellectual property protection.** Governments might regulate cross-border data flows as a way to protect intellectual property rights, including trademark, copyrights, and trade secrets.

  Regulatory access. Domestic regulators often require access to certain data for law-enforcement purposes. Some governments might require that data be stored domestically as a way to ensure access.

In addition, it is often maintained that policy makers might place conditions on cross-border data flows or require firms to store data domestically as a form of digital industrial policy (or digital protectionism). Autocratic regimes have also been accused of preventing cross-border data flows to curb free speech and as a means of political oppression (Fan and Gupta, 2018[34]).

Reflecting this range of motivations, and cultural and historical differences in policy approaches, governments around the world opt for different types of regulation to govern cross-border data flows. Some stipulate broad accountability principles with extraterritorial reach. Others require specific safeguards for cross-border transfers, including mandates that a destination country be whitelisted by domestic authorities

(though criteria vary across countries and are not always transparent), or that contracts exist between entities exchanging data (containing pre-approved clauses in some cases). Other regulations stipulate the review and approval of every transfer of data abroad. In addition to differences between regulations, they are applied to different types of data and sectors. And definitions and concepts can vary, such as on what constitutes personal information.

Regulations that promote trust online support data as an enabler of the global economy. But regulations can also be costly, especially when they are vague, fragmented, or lack transparency. Variation in the scope and application of rules between jurisdictions confront digital firms with a complex and uncertain global regulatory landscape. For example, attempts to provide a legal basis for transfers of personal data between the US and EU were struck down twice since 2015. Firms need a stable regulatory environment to make investment decisions and plans, and some worry that this confusing and shifting context could stunt economic opportunities. Some requirements can be technically challenging if not unfeasible, and small firms – including high-growth start-ups – can find compliance costs more difficult to absorb. This raises the possibility of even greater concentration of digital markets and decreasing business dynamism.

To address fragmentation and reduce challenges, international co-operation on "data free flow with trust" is key. There are foundations to build on, including the OECD Privacy Guidelines, which provide a baseline for privacy regulation; the Asia-Pacific Economic Cooperation, which has developed its own certification system for transferring data between participating economies; or the European Council's Convention 108, which provides rules on data-protection and transfers between parties. Some trade agreements contain binding provisions to keep data flowing between countries when protection frameworks are in place. Advancing interoperability of privacy frameworks has been a particular focus to allow countries with different privacy norms to continue to exchange data. Finally, privacy-enhancing technologies might enable the sharing and use of personal data, including across borders, with lower risks to privacy. Policy makers must assess these developments and identify next steps to get policies right for individuals and businesses.

4 Security: Fundamental enabler of the digital transformation, or its Achilles' heel?

As more parts of the economy come to rely on digital technologies, the stakes increase for digital security. Effective security enables confidence in and growth of the digital transformation. Unfortunately, the explosive pace of digital transformation to date has not come with a commensurate increase in the quality of security in devices and services. While some progress has been made to normalise good practice (e.g. coordinated vulnerability management, or security requirements for the Internet of Things), these baseline requirements have not been implemented by organisations at all scales. There is now an opportunity for policy makers worldwide to address these often international challenges by focusing on desired outcomes for the end-user and building on global Technical Standards and industry best-practices to strengthen interoperability.

The Internet of Things (IoT) – the conjunction of devices and objects connected to the Internet – embodies a wider challenge within digital security. Consumer IoT, also known as "smart" or "connected" products, expand the attack surface beyond traditional information and communications (ICT) technologies used by consumers, business and governments. Smart devices constitute a growing attack surface of insecure products that are adopted by consumers and integrated into networks. There were 7.7 billion IoT devices in 2019 (Statista, 2022[35]), and according to a recent survey, 78.4% of manufacturers of consumer IoT devices do not embed an internal process to address vulnerabilities (IoT Security Foundation, 2021[36]), which is critical for the on-going protection of the product and its user.

A relatively small number of nefarious actors have been able to capitalise on the digital transformation by embracing cybercrime business models that seek to evade conventional law enforcement. Ransomware has become a common threat affecting all types of businesses and organisations regardless of their size and location. In the US in 2021, operators of critical infrastructure filed 649 complaints to the FBI, and 14 of the 16 critical infrastructure sectors had at least one member fall victim to a ransomware attack (FBI, 2021[37]). Similarly, information systems have vulnerabilities related to how software is designed, developed, implemented and updated. Malicious actors develop, trade and use tools such as malware to exploit these vulnerabilities through incidents that harm businesses, governments and individuals, threaten critical activities, and undermine trust in the digital transformation.

The costs of an insecure digital ecosystem can be immense. Estimates for the potential global cost of cyberattacks have risen to USD 6 trillion per year (equal to the combined GDP of France and Germany) and rise every year (OECD, 2021[38]). Attackers look for digitally dependent victims. According to the CyberPeace Institute, 253 incidents in 32 countries in 2021 affected the healthcare sector, with an average of over 21 days in operational impact and over 13 million records affected (CyberPeace Institute, n.d.[39]).

Ideally, market forces ensure that products, including code (e.g. software, IoT devices, etc.) and related services (e.g. the cloud) are sufficiently secure, and that developers strengthen security in proportion to the risk faced by users and do so over the life cycle of the product. However, OECD analysis shows that

market failure prevent stakeholders from accurately valuing the digital security of products and services, and that market incentives alone are unlikely to fix gaps in digital security risk management (OECD, 2021[38]). In particular, the allocation of responsibilities for fixing vulnerabilities and improving security are unclear because of complex and opaque supply chains.

End-users, particularly small and medium-sized enterprises and consumers typically find it difficult to learn how much security is embedded by design in the products and services they purchase. Without this pressure, and in addition to complexities such as international supply chains, suppliers often neglect digital security as an "after thought", enabling malicious actors to use these products to launch attacks, including across borders. More broadly, there are misperceptions of digital security risk and misalignment of market incentives. In a 2020 survey, 28% of UK consumers said that they were not actively looking to buy an internet-connected product because of security fears (DCMS, 2020[40]).

Many of the challenges facing digital security (and digital transformation more broadly) are global. Supply chains are complex and international, posing challenges to legislators. Meanwhile, cloud and managed service providers offer services across borders, which can be vulnerable to malicious actors from anywhere. However, security researchers also work across borders and "safe harbour" legal frameworks must be designed based on internationally recognised principles to be effective.

5 Conclusion: A digital Bretton Woods? The role of the OECD in global digital governance

The Internet scaled to accommodate massive growth in users and devices worldwide (OECD, 2016[3]), and heralded an era of economic activity that is equally global. Digital transformation enables services, technologies and applications, and devices to span the globe. In a networked and interdependent world policy challenges are inherently international in scope, with effects rippling easily across borders.

However, efforts to manage policy challenges arising from online platforms, cross-border data flows and digital security have largely been conducted through national policies. Not only are such policies less likely to be effective, but the resulting fragmented landscape creates an uneven global playing field and unequal protection for consumers and businesses that benefit from the global economy.

The period after World War I was characterised by economic crises and increasing geopolitical tensions. Yet rather than opt for international co-operation, countries adopted policies that benefitted them at the expense of others, deepening the divisions. At the end of World War II, a select group of countries came together in Bretton Woods, in the US state of New Hampshire, to create a system of global institutions with the understanding that the benefits of a global economy could only be realised through co-operation.

Commentators increasingly invoke this wave of post-war multilateralism when calling for global digital policy frameworks. Although the terminology varies, there have been appeals for a 'Bretton Woods for digital policy' (Rockefeller Foundation, 2021[41]; Greenwald, 2020[42]; Clegg, 2021[43]; Tett, 2019[44]), a 'Digital Stability Board' (CIGI, 2019[45]) or a 'Digital Geneva Convention' (Microsoft, 2017[46]). Policy institutions have echoed the need for global digital policy frameworks, highlighting three characteristics: (1) the development of common, minimum international norms and principles; (2) better measurement and monitoring of digital technologies and issues; and (3) inclusive, multi-stakeholder involvement (World Bank, 2021[47]; United Nations, 2019[48]; UNCTAD, 2021[49]; Haksar et al., 2021[50]).

The OECD – with roots in this wave of multilateralism and expertise in digital policymaking – is well-placed to respond to these calls:

- **The OECD has shown longstanding leadership in digital policy issues, including international standards and policy frameworks**. In 1980, the OECD developed the *OECD Privacy Guidelines*, revised in 2013, which remain the global minimum standard for privacy and data protection codified in countries worldwide. The OECD also developed the first internationally agreed standards for digital security for growth and prosperity (OECD, forthcoming[13]; OECD, forthcoming[14]; OECD, forthcoming[15]; OECD, forthcoming[16]), and principles for data-access and sharing (OECD, 2021[11]), as well as the pioneering *OECD Artificial Intelligence Principles* (OECD, 2019[51]), and the *OECD Recommendation on Consumer Protection in E-Commerce* (OECD, 2016[9]). Implementation of these recommendations is reviewed regularly. Further, the OECD has expertise in policy areas affected by digital technologies and data – including taxation, competition, consumer protection, privacy, data governance, digital security, trade and financial and labour

markets – and it developed the first comprehensive integrated policy framework for the design and implementation of whole-of-government digital policies (OECD, 2020[52]).

- **The OECD is recognised for measuring, monitoring and assessing digital technologies and their economic and social effects**. The OECD leads international efforts to measure aspects of digital transformation, including digital trade (OECD-WTO-IMF, 2020[53]) and data (OECD, forthcoming[54]) in economic statistics and through the *Going Digital Measurement Roadmap* (OECD, 2022[55]). In monitoring the outcomes of the digital economy, the OECD developed tools and indicators to inform policymaking, including the *OECD Going Digital Toolkit* and the *OECD AI Policy Observatory*. Further, the OECD examines and assesses the effects of emerging digital technologies, such as artificial intelligence and blockchain (OECD, 2022[56]).
- **The OECD provides a model for inclusive, global and multi-stakeholder dialogue on digital economy policy**. As a forum for exchanging ideas and good practices among over 100 countries, the OECD brings together decision- and policy makers from around the world to share lessons, identify best practices, and develop evidence-based policies for an evolving digital world. Digital-economy policy discussions at the OECD follow a multi-stakeholder model where the experience and expertise of business, trade unions, civil society, and the Internet technical community are given a platform to enable the digital transformation to flourish and embed security considerations. In addition, the OECD's work on international tax reform in the digital age highlights its ability to convene countries for consensus on complex, cross-cutting issues raised by the digital transformation (OECD, 2022[57]). The *OECD Global Forum on Competition* (OECD, 2022[58]) and the *OECD Global Forum on Digital Security for Prosperity* (OECD, 2022[59]) are other examples of multilateral, multidisciplinary engagement led by the OECD.

International institutions and policy organisations recognise the need for global digital policy frameworks. Empowered by countries, and in dialogue with relevant international organisations, the OECD can build on its established role, institutional know-how, wealth of analytical tools, and proven capacity to work with countries and stakeholder groups to set an ambitious path for digital policymaking, and to manage the policy issues associated with an interdependent and digital global economy and society.

References

Aaronson, S. (2019), "What Are We Talking about When We Talk about Digital Protectionism?", *World Trade Review*, Vol. 18/4, pp. 541-577, https://doi.org/10.1017/S1474745618000198. [33]

Bajgar, M. et al. (2019), "Industry Concentration in Europe and North America", *OECD Productivity Working Papers*, No. 18, OECD Publishing, Paris, https://doi.org/10.1787/2ff98246-en. [24]

Bajgar, M., C. Criscuolo and J. Timmis (2021), "Intangibles and industry concentration: Supersize me", *OECD Science, Technology and Industry Working Papers*, No. 2021/12, OECD Publishing, Paris, https://doi.org/10.1787/ce813aa5-en. [26]

Baldwin, R. (2017), *The Great Convergence*, Harvard University Press, https://doi.org/10.4159/9780674972667. [31]

Burdon, T. (2021), "The role of online marketplaces in enhancing consumer protection", *OECD Going Digital Toolkit Notes No. 7*, OECD Publishing, Paris, https://doi.org/10.1787/ddca0e2e-en. [20]

Calvino, F. and C. Criscuolo (2019), "Business dynamics and digitalisation", *OECD Science, Technology and Industry Policy Papers*, No. 62, OECD Publishing, Paris, https://doi.org/10.1787/6e0b011a-en. [25]

Casalini, F. and J. López-Gonzalez (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Paper*, No. 220, OECD, Paris, https://doi.org/10.1787/b2023a47-en (accessed on 4 March 2022). [32]

CIGI (2019), *Digital Platforms Require Global Governance Frameworks*, https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework/. [45]

Clegg, N. (2021), *A Bretton Woods for the Digital Age can Save the Open Internet*, https://www.afr.com/technology/a-bretton-woods-for-the-digital-age-can-save-the-open-internet-20211115-p5994h. [43]

Corrado, C. et al. (2021), "New evidence on intangibles, diffusion and productivity", *OECD Science, Technology and Industry Working Papers*, No. 2021/10, OECD Publishing, Paris, https://doi.org/10.1787/de0378f3-en. [63]

Cory, N. and L. Dascoli (2021), *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology & Innovation Foundation, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost (accessed on 5 April 2022). [61]

CyberPeace Institute (n.d.), *Cyber Incident Tracer #HEALTH*, https://cit.cyberpeaceinstitute.org/explore (accessed on 11 July 2022). [39]

DCMS (2020), *Evidencing the Cost of the UK Government's Proposed Regulatory Interventions for Consumer IoT*, UK Department for Digital, Culture, Media & Sport, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf (accessed on 11 July 2022). [40]

Fan, Z. and A. Gupta (2018), *The Dangers of Digital Protectionism*, https://hbr.org/2018/08/the-dangers-of-digital-protectionism (accessed on 6 October 2022). [34]

FBI (2021), *Internet Crime Report*, U.S. Federal Bureau of Investigation, Washington, DC, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed on 11 July 2022). [37]

Furman, J. et al. (2019), *Unlocking digital competition: Report from the Digital Comeptition Expert Panel*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf. [22]

Gierten, D. and M. Lesher (2022), "Assessing National Digital Strategies and Their Governance", *OECD Digital Economy Papers*, No. 324, OECD Publishing, Paris, https://doi.org/10.1787/baffceca-en (accessed on 11 July 2022). [4]

Gray, M. (1996), *Web Growth Summary*, https://www.mit.edu/people/mkgray/net/web-growth-summary.html (accessed on 17 October 2022). [2]

Greenwald, M. (2020), *A new era in financial diplomacy: The third evolution of Bretton Woods*, https://www.atlanticcouncil.org/blogs/new-atlanticist/a-new-era-in-financial-diplomacy-the-third-evolution-of-bretton-woods/. [42]

Haksar, V. et al. (2021), *Toward a Global Approach to Data in the Digital Age*, https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/10/06/Towards-a-Global-Approach-to-Data-in-the-Digital-Age-466264. [50]

Internet Live Stats (2022), *Total number of Websites*, https://www.internetlivestats.com/total-number-of-websites/ (accessed on 8 July 2022). [60]

IoT Security Foundation (2021), *The Contemporary Use of Vulnerability Disclosure in IoT (Report 4)*, https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf (accessed on 11 July 2022). [36]

McFadden, J. et al. (2022), "The digitalisation of agriculture: A literature review and emerging policy issues", *OECD Food, Agriculture and Fisheries Papers*, No. 176, OECD Publishing, Paris. [62]

Microsoft (2017), *The need for a Digital Geneva Convention*, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. [46]

Netcraft (2022), *Web Server Survey*, https://news.netcraft.com/archives/category/web-server-survey/ (accessed on 17 October 2022). [1]

OECD (2022), "Dark Commercial Patterns Online", *OECD Digital Economy Papers,* No. 336, https://doi.org/10.1787/44f5e846-en. [29]

OECD (2022), *Global Blockchain Policy Centre*, https://www.oecd.org/daf/blockchain/. [56]

OECD (2022), *International collaboration to end tax avoidance*, https://www.oecd.org/tax/beps/. [57]

OECD (2022), *OECD Global Forum on Competition*, https://www.oecd.org/competition/globalforum/. [58]

OECD (2022), *OECD Global Forum on Digital Security for Prosperity*, https://www.oecd.org/digital/global-forum-digital-security/about/. [59]

OECD (2022), *OECD Handbook on Competition Policy in the Digital Age*, https://www.oecd.org/daf/competition/oecd-handbook-on-competition-policy-in-the-digital-age.pdf. [21]

OECD (2022), "The Evolving Concept of Market Power in the Digital Economy", *OECD Competition Policy Roundtable Background Note*, https://www.oecd.org/daf/competition/the-evolving-concept-of-market-power-in-the-digital-economy-2022.pdf. [27]

OECD (2022), "The OECD Going Digital Measurement Roadmap", *OECD Digital Economy Papers*, No. 328, OECD Publishing, Paris, https://doi.org/10.1787/bd10100f-en. [55]

OECD (2022), "The role of online marketplaces in protecting and empowering consumers: Country and business survey findings", *OECD Digital Economy Papers*, No. 329, OECD Publishing, Paris, https://doi.org/10.1787/9d8cc586-en. [6]

OECD (2021), *Communique on Product Safety Pledges*, https://one.oecd.org/document/DSTI/CP/CPS(2021)8/FINAL/en/pdf. [30]

OECD (2021), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers*, No. 307, OECD Publishing, Paris. [19]

OECD (2021), "Ex Ante Regulation and Competition in Digital Markets", *OECD Competition Committee Discussion Paper*, https://www.oecd.org/daf/competition/ex-ante-regulation-and-competition-in-digital-markets-2021.pdf. [28]

OECD (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463 (accessed on 21 April 2022). [11]

OECD (2021), "Smart Policies for Smart Products: A Policy Maker's Guide to Enhancing the Digital Security of Products", *STI Policy Note*, OECD Publishing, Paris, https://www.oecd.org/digital/smart-policies-for-smart-products.pdf (accessed on 11 July 2022). [38]

OECD (2021), *Strengthening Economic Resilience Following the COVID-19 Crisis: A Firm and Industry Perspective*, OECD Publishing, Paris, https://doi.org/10.1787/2a7081d8-en. [23]

OECD (2021), "Understanding the digital security of products: An in-depth analysis", *OECD Digital Economy Papers*, No. 305, OECD Publishing, Paris. [18]

OECD (2020), "Going Digital integrated policy framework", *OECD Digital Economy Papers*, No. 292, OECD Publishing, Paris, https://doi.org/10.1787/dc930adc-en. [52]

OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, https://doi.org/10.1787/53e5f593-en. [7]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [51]

OECD (2019), *Unpacking E-commerce: Business Models, Trends and Policies*, OECD Publishing, Paris, https://doi.org/10.1787/23561431-en. [8]

OECD (2016), "Digital Convergence and Beyond: Innovation, Investment and Competition in Communication Policy and Regulation for the 21st Century"*, OECD Digital Economy Papers*, No. 251, OECD Publishing, Paris, https://doi.org/10.1787/5jlwvzzj5wvl-en. [3]

OECD (2016), *Recommendation of the Council on Consumer Protection in E-commerce*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422. [9]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [12]

OECD (forthcoming), "Data shaping firms and markets", *OECD Digital Economy Papers*, OECD Publishing, Paris. [5]

OECD (forthcoming), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, OECD Publishing, Paris. [10]

OECD (forthcoming), "Measuring the value of data and data flows", *OECD Digital Economy Papers*, OECD Publishing, Paris. [54]

OECD (forthcoming), *Policy Framework on Digital Security*, OECD Publishing, Paris. [17]

OECD (forthcoming), *Recommendation on Digital Security Risk Management*, OECD. [13]

OECD (forthcoming), *Recommendation on National Digital Security Strategies*, OECD. [14]

OECD (forthcoming), *Recommendation on the Digital Security of Products and Services*, OECD. [15]

OECD (forthcoming), *Recommendation on the Treatment of Digital Security Vulnerabilities*, OECD. [16]

OECD-WTO-IMF (2020), *Handbook on Measuring Digital Trade*, https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf. [53]

Rockefeller Foundation (2021), *A Bretton Woods for AI: Ensuring Benefits for Everyone*, https://www.rockefellerfoundation.org/blog/a-bretton-woods-for-ai-ensuring-benefits-for-everyone/;. [41]

Statista (2022), *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 11 July 2022). [35]

Tett, G. (2019), *Do we need an IMF to regulate the internet?*, https://www.ft.com/content/4526982e-60a0-11e9-b285-3acd5d43599e (accessed on 20 February 2022). [44]

UNCTAD (2021), *Digital Economy Report 2021*, https://unctad.org/page/digital-economy-report-2021. [49]

United Nations (2019), *The Age of Digital Interdependence*, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf. [48]

World Bank (2021), *World Development Report*, World Bank Publishing, Washington DC, https://www.worldbank.org/en/publication/wdr2021. [47]

Notes

[1] Product safety pledges commit platforms to actions that go beyond their legal obligations to protect consumers from unsafe products (such as by removing listings for unsafe products within a certain time period upon notification by a government authority). The OECD's Working Party on Consumer Product Safety recently released a communiqué calling for governments to develop more such pledges, with marketplaces incorporating four commitments to encourage consistency internationally (OECD, 2021[30]).