'Splinternets': Addressing the renewed debate on internet fragmentation

Clément Perarnaud, Julien Rossi, Francesca Musiani, Lucien Castex

European Parliament

'Splinternets': Addressing the renewed debate on internet fragmentation

STUDY

Panel for the Future of Science and Technology

EPRS | European Parliamentary Research Service

Scientific Foresight Unit (STOA)
PE 729.530 – July 2022

EN

'Splinternets': Addressing the renewed debate on internet fragmentation

Recent events have multiplied concerns about potential fragmentation of the internet into a multitude of non-interoperable and disconnected 'splinternets'. Composed of thousands of compatible autonomous systems, the internet is by definition technically divided. Yet, the internet was also designed to be an open and global technical infrastructure. The unity and openness of the internet appear to be under great pressure from political, commercial and technological developments.

This report explores the implications of the EU's recent policies in this field as well as the opportunities and challenges for EU Member States and institutions in addressing internet fragmentation. It underlines how recent EU legislative proposals – on the digital services act, digital markets act, artificial intelligence act, and NIS 2 Directive – could help to address patterns of fragmentation, but also have limitations and potentially unintended consequences.

Four possible strategies emerge: stay with the status quo, embrace fragmentation, resist patterns of divergence, or frame discussions as a matter of fundamental rights.

AUTHORS

This study has been written by Clément Perarnaud (Brussels School of Governance – Vrije Universiteit Brussel), Julien Rossi (COSTECH – Université de technologie de Compiègne and PREFICS – Université Rennes 2), Francesca Musiani (CIS – CNRS) and Lucien Castex (IRMECCEN – Université Sorbonne Nouvelle), at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

Acknowledgements

The authors are indebted to the individuals (and their organisations) who contributed their time and expertise to this report: Amelia Andersdotter, Sébastien Bachollet, Farzaneh Badii, Stéphane Bortzmeyer, Chris Buckbridge, Alissa Cooper, Ross Creelman, William Drake, Jim Dratwa, David Frautschy, Lise Fuhr, Valentin Grimaud, Alexandra Laffitte, Riccardo Nanni, Mark Nottingham, Niels ten Oever, Maarit Palovirta, Oriane Piquer-Louis, Julia Pohle, Lars Steffen, Adrien Tournier, Peter Van Roste and Rigo Wenning. They are grateful to Nizar Larabi and Simon Bourdieu-Apartis, who provided administrative support for CNRS at the Meudon-Ile-de-France delegation and at Centre Internet et Société, respectively. Finally, they thank the Working Group on Internet Governance and Regulation of the CIS research network, and to the Global Internet Governance Academic Network (Giga-Net) with whose members they have had fruitful exchanges throughout the research and writing for this report.

ADMINISTRATOR RESPONSIBLE

Philip Boucher, Scientific Foresight Unit (STOA)

To contact the publisher, please e-mail stoa@ep.europa.eu

LINGUISTIC VERSION

Original: EN

Manuscript completed in June 2022.

PE 729.530
ISBN: 978-92-846-9621-5
doi:10.2861/183513
QA-09-22-292-EN-N

http://www.europarl.europa.eu/stoa (STOA website)
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

Recent debates around the growing fragmentation of the internet and the emergence of 'splinternets' have raised the issue of an increasing divergence of internet standards and protocols.

By its very nature, the internet is a collection of fragmented networks, but these networks and the services provided on top are nonetheless able to provide the experience of a seamless, open, united and interconnected online public sphere. This is in large part due to properties of interoperability and interconnection provided by open standards and formats, standardised by bodies such as the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C). The domain name system (DNS) is also pivotal in supporting this one, global internet. However, several factors may disrupt this fine balance between divergence and convergence of the internet as a 'network of networks'. Users are threatened by 'enclosure' into technological walled gardens, and by the creation of splinternets that can no longer interact with other networks, not only at the application layer, but also at the layers of protocols and physical infrastructures, further removed from the users' perception and reach'. Fragmentation can be total or partial. It can happen at the transport layer of the network, or because of incompatible applications and formats. It can also be caused by technological, political or commercial factors.

Indeed, forms of fragmentation and divergence can be observed at specific nodes of certain layers of the internet, with sometimes great implications for its global architecture and the compatibility of its systems, while the experience of internet users also appears to diverge increasingly based on profile, location and devices.

The layered and distributed architecture of the internet, means that patterns of fragmentation can take various forms and their observation requires a dynamic and graduated approach. Indeed, a wide constellation of actors and processes constantly shape the technical arrangements on which the internet relies, and have direct effects on the public sphere resulting from this infrastructure and its uses.

Drawing on an analysis of recent patterns of divergence of internet standards and protocols, differentiated in function of their underlying technological, commercial and political root causes, this report explores the implications of EU's recent policies in this field as well as the opportunities and challenges for EU Member States and institutions in addressing the so-called phenomenon of internet fragmentation.

Building on the latest scholarship in the field of internet governance, it identifies and illustrates core threats to the development of a unified internet. These include a range of processes and developments, such as technical factors fuelling forms of technical splintering, a reduction in the flexibility of networks (or internet ossification), growing organisational concentration in internet governance, consolidation of the internet architecture and digital economy, and the process of alignment of the internet with territorial borders.

In relation to these challenges, the EU's legislative agenda can be seen as a driver for positive opportunities, but also as a potential catalyser for the worsening of the very same threats. Both internally and externally, the EU has repeatedly committed to promote the development of a single, open, neutral, free, secure and un-fragmented network, while adopting a more strategic approach to the making process of internet standards and protocols. The report underlines how ongoing EU legislative proposals – on the digital services act, the digital markets act, the artificial intelligence act, and the NIS 2 Directive – have the potential to help address patterns of divergence, but also describes how their limitations and unintended consequences need to be addressed in order to ensure the coherence and consistency of the EU's action in this increasingly strategic field.

Through a variety of policy initiatives and instruments, the European Union also affects this balance. Despite the Open Internet Regulation (2012/2120/EU), the EU's overall approach lacks consistency. Some measures affect connectivity negatively, often in the name of digital sovereignty: examples of this tendency are the drive towards a sovereign, regional European cloud, which would allow the data of European users to be shared and circulated only within Europe and not be subject to the United States' more lenient privacy laws. Other measures are supportive of an open and universal internet, like those favouring competition between private actors, enshrining principles of network neutrality or promoting interoperability and data portability, or supporting, through dedicated research funding programmes, the elaboration of distributed and decentralised network architectures. This indecisiveness can be explained in part by the fact that – somewhat surprisingly – internet fragmentation is still in its early stages of political problematisation, despite having been the topic of regular speculations and occasional fears among a few actors.

This report reviews several recent or current policy initiatives within the framework of the digital single market (DSM), and analyses key features of existing legislation affecting this tension between fragmentation and unity. We outline several possible strategies to promote a consistent way for the EU to approach this subject matter: maintaining the status quo, embracing fragmentation, or consistently fighting fragmentation. We review each of these scenarios against rules laid out in international trade law and the EU Treaties, looking especially at the compatibility of each scenario with requirements laid out by the EU's Charter of Fundamental Rights, but also the impact each scenario may have on the continued functioning of the internet.

Each of the three scenarios had significant drawbacks from the point of view of the EU's legal obligations in general, and fundamental rights in particular, or were insufficiently consistent. As such, we also outline a fourth option: framing the debate on internet fragmentation as a matter of fundamental rights, composed of both negative and positive obligations. We propose a framework that applies a proportionality test to each limitation to the unity of the internet, ensures that private actors do not limit these same rights and freedoms, and promotes accountability while accepting limitations to the ability of state-actors to impose standards and manage telecommunications infrastructure as part of a modern system of checks and balances in the network society.

The report is based upon a number of interviews of key experts and stakeholders to gather their experience and opinions. We have paid particular attention to include a variety of standpoints with a multi-stakeholder perspective including institutional representatives, academics, technical community key actors, civil society, private sector, and associations supporting online civil liberties. In addition to individual interviews, several of these experts were gathered in a day of online workshop on 15 February 2022, which included a research-oriented and a practitioner/stakeholder-oriented session.

Table of contents

1. Introduction 1

1.1. Key definitions 3

1.2. An introduction to standardsetting organisations 5

1.3. The politics of standards 8

2. Methodology 9

3. Patterns of divergence of internet standards and protocols 11

3.1. Technological factors 14

3.1.1. Network address translation: From IPv4 to IPv6 14

3.1.2. Protocol competition at the transport-layer: The development of TLS 1.3 and ETS 15

3.1.3. The lack of universal acceptance for internationalised domain names 16

3.2. Commercial factors 17

3.2.1. The case of the deployment of Quick UDP internet connections (QUIC) 18

3.2.2. The concentration of the DNS resolver market 19

3.2.3. Ad-based profiling and the FLoC proposal 21

3.2.4. Incompatibilities at the application-layer: the case of web browsers' engines 22

3.3. Political factors 23

3.3.1. The internet's increasing alignment with territorial borders 24

3.3.2. National approaches towards internet standardisation: The case of China 24

3.3.3. National approaches towards internet standardisation: The case of Russia 26

4. The EU and internet fragmentation 30

4.1. The EU and internet standardisation 31

4.2. Current EU approach and legislative developments 33

4.2.1. Digital Markets Act (2020) 35

4.2.2. Digital Services Act (2020) 36

4.2.3. NIS 2 Directive (2020) 39

4.2.4. Artificial Intelligence Act (2021) 41

5. Challenges and opportunities 43

6. Policy options 47

6.1. Introduction 47

6.1.1. Framework for the policy options 47

6.1.2. General considerations guiding the assessment of the policy options 48

6.2. Comparing comprehensive strategic options on internet fragmentation 49

6.2.1. Maintaining the status quo 49

6.2.2. Embracing fragmentation 50

6.2.3. Consistently fighting fragmentation 53

6.2.4. Towards fragmentation that is 'necessary in a democratic society' 54

6.3. Assessment of the policy options 56

7. Conclusion 58

References 59

Appendices 65

Table of figures

Figure 1: The traditional TCP/IP protocol suite 6

Figure 2: Internet governance-related institutions at regional and global levels 7

Figure 3: Selection of Standards and Standard Development Organisations (SDOs) 8

Figure 4: Typology of fragmentation processes 11

Table of tables

Table 1: Legislative dossiers under study 34

A1. Technologies and protocols under study and their role in internet divergence and convergence. 65

A2. Key organisations in the development of a selection of Internet standards and protocols. 66

A3. EU legislative dossiers under study and their relevance to Internet fragmentation. 67

List of abbreviations

3GPP	3rd Generation Partnership Project
AI	Artificial intelligence
AS	Autonomous systems
BEUC	Bureau Européen des Unions de Consommateurs
CDNs	Content delivery networks
CDT	Center for Democracy & Technology
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERN	European Organization for Nuclear Research
CJEU	Court of Justice of the EU
CMA	United Kingdom's Competition and Markets Authority
CNCDH	French Commission nationale consultative des droits de l'homme
CSS	Cascading style sheets
DII	Decentralised internet infrastructure
DMA	Digital Markets Act
DNS	Domain name system
DNT	Do not track
DSA	Digital Services Act
DSM	Digital single market
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EECC	European Electronic Communication Code
EFF	Electronic Frontiers Foundation
ESO	European standards Organisations
ESS	European standardisation system
ETS	Enterprise transport security
ETSI	European Telecommunications Standards Institute
EU	European Union
EUID	Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity
FLoC	Federated learning of cohorts

GDPR	General Data Protection Regulation
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technologies
IDNA	Internationalising domain names in applications
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IoT	Internet of things
IP	Internet Protocol
ISC	Internet Systems Consortium
ISO	International Organisation for Standardisation
ISP	Internet service provider
IT	Information technology
ITRE	European Parliament's Committee on Industry, Research and Energy
ITU-T	Telecommunication Standardization Sector of the ITU
IXP	Internet exchange point
MEP	Member of the European Parliament
MIT	Massachusetts Institute of Technology
NAPTs	Network address and port translators
NAT	Network address translations
NDNS	National domain name system
NIS	Network and information system security
NSA	National Security Agency
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organization for Economic Co-operation and Development
OEWG	Open ended working group
OSI	Open systems interconnection
PPTP	Point-to-Point Tunneling Protocol
QUIC	Quick UDP Internet Connections protocol
RFC	Request for comments

RIPE NCC	Réseaux IP Européens Network Coordination Centre
ROAM	Rights, open, accessible to all, multi-stakeholder
RSO	Root server operators
SDO	Standard developing organisation
SORM	Systems for operative investigative activities
SSL	Secure sockets layer
TCI/IP	Transmission Control Protocol/Internet Protocol
TLDs	Top-level domains
TLS	Transport layer security
TSAG	ITU's Telecommunication Standardization Advisory Group
UNESCO	United Nations Educational, Scientific and Cultural Organization
URL	Uniform resource locators
VPN	Virtual private network
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WTO	World Trade Organisation

1. Introduction

The Covid-19 pandemic has demonstrated, beyond reasonable possible doubt, the vital character of information and communication technology (ICT) and our collective reliance on computer networks for the continuity of vital public services, economic activities and social relationships. Education, business meetings, and even birthday parties have all had to rely on the internet during the multiple lockdowns occurring between March 2020 and today, in Europe and elsewhere in the world.

Despite initial worries about the internet faced with such a sudden and strong increase in demand, the internet as an infrastructure proved to be remarkably resilient. Shifts in Internet traffic patterns, due to the 'massification' of remote work for instance, had caused fears of a global outage or the significant degradation of the quality of users' experience and service performance.

The decentralised nature of the internet was designed to improve its resilience. Resilience is usually defined as the capacity of a network to 'provide and maintain an acceptable level of service in the face of faults and challenges to normal operation' (Dawit, 2020). Yet this resilience should not be taken for granted. When key critical assets in the infrastructure fail, connectivity is affected on a global scale. A global outage of many websites, including that of the British government, due to the failure of a single content delivery network provider, took place in June 2021[1]. Earlier, in August 2019, users of Google cloud services experienced difficulties because of an outage of that company's single sign-on system[2]. Patterns of centralisation of the internet have thus led to worries over its continued resilience.

The Internet was also designed for its openness. Though a constant feature of Internet governance discussions, this notion of openness is complex and multi-dimensional. For instance, openness at the technical level is expected to 'increase when openly available protocols are used consistently to receive and send data flows across interoperable layers of the Internet' (Box & West, 2016). On the social and economic sides, regulations on net neutrality have been aimed at defending openness, by making sure that all users and businesses are treated in the same way on the network, even if they are new entrants on digital markets. As such, the internet is a global network of interoperable networks. They are able to communicate with each other across nations, and despite being made up of a high variety of physical equipment and software, because all the nodes in the network speak a common language made of protocol and format standards. This infrastructure has created a global online public sphere and marketplace where ideas, services, data and digital goods are exchanged. The unity of the internet can thus be defined as the technical capacity to communicate in a frictionless manner across all networks constituting the internet, thereby supporting a virtual public sphere where everyone has equal access regardless of geographical location or any other form of discrimination.

Both the unity and the openness of the internet are now under pressure from both political, economic and technological developments. Some state actors, like Russia and China, are attempting to limit access of their citizens to the global contents of the global online public sphere, and align their IT infrastructure to their national borders. Some private actors are limiting interoperability, either on purpose or by accident, by promoting standards that are not interoperable, thereby enclosing their users in technological silos. In addition, in the absence of rules restricting planned obsolescence or encouraging retro-compatibility, citizens and consumers with limited financial

[1] For more, see: https://www.bloomberg.com/news/articles/2021-06-08/explaining-cdns-and-why-big-websites-crash-together-quicktake.

[2] For more, see: https://www.zdnet.com/article/cant-log-in-to-google-services-reported-down-for-some-users/.

resources may struggle to keep their equipment up-to-date and compatible with current infrastructure.

Although the unicity and coherence of Europe's digital space has been a subject of concern for the EU, the past few years, and especially the last months, have seen many developments in the area of Internet Governance at the national, regional and global levels, many of which directly relate to the topic of Internet unity or fragmentation.

- For example, the July 16 2020 decision of the Court of Justice of the EU (CJEU) that has come to be colloquially known as Schrems II (ruling that the EU-US Privacy Shield was invalidated due to concerns about US state surveillance) was followed by decisions from the Austrian and French Data Protection Authorities (DSB and CNIL, respectively) stating that data transfers in the frame of Google Analytics were illegal (NOYB 2022, CNIL 2022).
- February 2022 saw the launch of the first coordinated enforcement action of the European Data Protection Board (EDPB): 22 supervisory authorities will launch investigations into the use of cloud-based services by the public sector in the coming months (EDPB 2022).
- Earlier in February, Facebook and Instagram made the headlines when parent company Meta in its annual report to the US Securities and Exchange Commission stated that it may have to leave the European space if regulators did not remedy a 'legal ambiguity' over transatlantic data transfers considering that processing user data between countries is key for targeted advertising (Nix 2022).
- A proposal for a Data Act legislation (defining the rules for sharing data, conditions for access by public bodies, international data transfers, cloud switching and interoperability in the European digital space) was officially published on the 23rd of February (COM 2022 68 Final).
- Early February, a proposal for an EU regulation amending Regulation (EU) No 1025/2012 as regards the decisions of European standardisation organisations concerning European standards and European standardisation deliverables was put forward.
- On 12 January 2022, the EU Commission launched a tender entitled 'Equipping backbone networks with high-performance and secure DNS resolution infrastructures' (DNS4EU), with the aim to creating a recursive DNS service EU-based, which includes a potentially sensitive mandate to filter content and create 'liar DNSs': lawful filtering based on legal requirements in the EU or in national jurisdictions of Member states and optional additional services (e.g. parental control) (Howell 2022), one difficulty being that what is legal in one state may be forbidden in another (for example, communist symbols are forbidden in Hungary, but are used by websites of political parties that have elected officials in several European countries).
- Initiatives related to Internet sovereignty as a possible cause of fragmentation happen worldwide. For example, in February 2021, Cambodia introduced a gateway to its national Internet (NIG), a system aimed at funnelling all international Internet connections through a single entry point, with the alleged aim of preventing online crime and promoting 'national interests' (France 24, 2022). This happens in a more global scenario of initiatives aiming at strengthening national Internets, including the well-studied cases of Russia and China.
- According to Netblocks, after February 25, following the invasion of Ukraine by Russian armed forces, several areas of Ukraine have experienced difficulties in accessing the internet (NetBlocks 2022a), and Roskomnadzor, the telecommunications regulator of the Russian Federation, has limited access to Facebook and Twitter (NetBlocks 2022b). On May 11, Facebook and Instagram were

blocked in the self-proclaimed republic of Donetsk, due to Meta, Facebook and Instagram's parent company, being considered as 'extremist' in Russia[3].

- On March 25, the European Commission and the United States announced a new Trans-Atlantic Data Privacy Framework, to replace Privacy Shield, which had been declared invalid by the CJEU in May 2020.

These new developments are stoking concerns among some that risks of seeing a fragmentation of the internet, which used to be widely dismissed by many experts due mainly to the network effects created by the internet and its role as a centrepiece infrastructure for the functioning of modern economies. Although fragmentation is usually portrayed as being a consequence of actions taken by states such as Russia or China, the European Union is also implementing policies that have an effect, some of which, but not all of which, being in the direction of a more united Internet.

Thus, this report aims at providing a review on the current divergence of Internet standards and protocols, and connect it with ongoing legislative negotiations at the European Union (EU) level.

The first part of this report introduces the key terms, describes the work of Internet standards-setting organisations and reflects on the processes and politics shaping Internet standards. Following the description of the methodological approach of this study, the next section consists in an analysis of recent patterns of fragmentation of Internet standards and protocols, differentiated by their underlying root causes. Though interdependent, it first focuses on technical factors, followed by a review of commercial and political factors. This first part will investigate patterns of technical splintering of Internet standards and protocols, taking into account both their formulation and deployment. These patterns and threats to Internet's unity and openness include transport protocol competition (TLS 1.3), Network Address Translation (Ipv6) and the lack of acceptance for internationalised domain names. The second part explores commercial factors, focusing mainly on the accelerating process of Internet consolidation (QUIC, DNS resolvers, FloC, Blink). The third part investigates the internet's alignment with national borders, looking in particular at national approaches from China and Russia, bearing in mind of the implications of the war in Ukraine.

The EU approach towards Internet standardisation and current negotiations in relation to the identified threats to Internet's unity and openness are then discussed. This section presents a brief description of the EU's history in engaging with Internet standardisation and explores the EU's current approach in relation to Internet fragmentation, through the analysis of four recent legislative proposals presented by the European Commission since 2020. The analysis looks specifically at the recently proposed EU's DSA, DMA, AI Regulation and NIS 2 directive. The next section identifies a number of challenges and opportunities for the EU in the context of ongoing and future legislative negotiations in relation to the divergence of Internet standards and protocols. The final part of the report considers various policy options in addressing these patterns, proposing a framework to test them in relation to their impact on the unity of the internet and fundamental rights.

1.1. Key definitions

The following glossary defines the key terms used in the study.

The Internet may be defined in two different ways. This word both refers to a **technical infrastructure**, and a **social space** (Abbate, 2017). Technically, the internet is defined by the Internet Engineering Task Force as 'a large, heterogeneous collection of interconnected systems that can be used for communication of many different types between any interested parties

[3] https://www.moscowtimes.ru/2022/05/11/v-dnr-zablokirovali-facebook-i-instagram-a20286.

connected to it' (Alvestrand, 2004). It is not one network, but a network of interconnected networks. Each individual network is called an 'autonomous system, which may have its own internal rules. Usually, autonomous systems are networks owned by Internet Service Providers (ISPs). These networks communicate with each other thanks to a common set of open standards, the most important of which being the Internet Protocol (IP). Content is shared across the networks, and across social and political boundaries, thanks to this common set of protocol and content format standards. Applications of the internet include the World Wide Web, electronic mail (e-mail), voice-over-IP or even payment services. As a social space, Félix Tréguer (2019) defines the internet as a public sphere resulting from this infrastructure and its uses. As social space, the internet is synonymous with the concept of cyberspace and comes from the imaginary of 1980' science fiction. It is the content users may access, produce and share using devices connected to one of the interconnected networks constituting the internet, and the human and social experience produced by this use.

The **World Wide Web**, or the **Web**, is an application of the internet. In other words, it is one of the uses that can be made of Internet as a communication infrastructure. Its name is derived from the idea that it is constituted by the web of documents linked together by hyperlinks. Initially, the Web was based upon three specifications: documents were all written in HyperText Markup Language (HTML), transferred using the HyperText Transfer Protocol (HTTP) and links were represented as URLs (Uniform Resource Locators) (Alvestrand & Wium Lie, 2009). The Web is typically accessed through a web browser, such as Mozilla Firefox or Google Chrome.

Internet universality is a concept launched by the United Nations Educational, Scientific and Cultural Organization (UNESCO) in 2013. Since 2015, UNESCO has developed an indicator framework to assess Internet universality based on four key principles, known as ROAM (Rights, Open, Accessible to all, Multistakeholder). Internet universality is often described as opposite to the concept of internet fragmentation (DeNardis, 2016).

Internet fragmentation is a broad and contested concept. This term is used in the academic literature and policy circles to refer to a wide range of phenomenon and patterns, such as the complete disconnection of systems from the global Internet (*technical fragmentation*) or manifestations of variations in Internet users' experiences when accessing online content (*content fragmentation*). As a global network of compatible autonomous systems, the internet is by definition connected, yet structurally fragmented into various segments. The notion of Internet fragmentation indeed embeds a paradox, as it conceptualizes the internet as an un-fragmented 'pre-existing whole' (Dratwa, 2009). Our definition of **technical fragmentation** is that it is the result of choices that intentionally or unintentionally break, restrict or suspend technical connectivity between a part of the internet and the rest of the network. Milton Mueller instead defines the technical fragmentation of the internet as the 'intentional defection from the global Internet, led by a group of actors capable of taking with them a substantial segment of the world's population […] which must succeed in establishing effective technical incompatibilities between their part of the Internet and the other part(s); and these incompatibilities must be both sustainable over a significant period of time and able to obstruct communications among parties that are willing to communicate' (Mueller, 2017, p. 43). This sets the bar rather high, and many elements in this definition exclude events that could be construed as fragmentation without any apparent reason. For instance, technical fragmentation may be the unintended by-product of divergent technological choices. It may only isolate a non-significant part of the population, and may be only temporary. Many concepts are used to illustrate the notion of Internet fragmentation and its implications, such as the term '**splinternet**', which designates a part of the internet that would secede and become inaccessible to the other nodes, due to either technological or political reasons. Similarly, '**balkanisation of the internet**' is an expression with negative connotation, used to characterize patterns of divisions leading to smaller, incompatible units. The process of fragmentation can apply both to the internet as infrastructure, and to the internet as public space. Indeed, in addition to

technical fragmentation as such, **content** fragmentation can also occur where connectivity is maintained at a technical level, but users are still restricted in their practical access to content. This may happen when, for example, a website can still be reached through its IP address, but has had its corresponding entry deleted from Domain Name System (DNS) servers used by a user's ISP, requiring the user to take specific action to restore access.

Alignment is a term related to fragmentation proposed by Milton Mueller which describes the 'collapse of the Internet's open-ended and expanding structure of 50,000+ Autonomous Systems into a structure that conforms to the numerically smaller, more controlled and concentrated system of sovereign states' (Mueller, 2017). Milton Mueller compares alignment to the 'digital equivalent of building customs checkpoints, tariffs, and roadblocks into the network' (Mueller, 2020). Advocates of this approach oppose the self-determination of the internet, which is a process whereby a multi-stakeholder process takes key decisions on the functioning of the internet without regard to nation-state borders.

The **consolidation of the internet** is a process of 'increasing control over Internet infrastructure and services by a small set of organizations' (Arkko, 2020). It is expected to affect traffic flows, services and systems that are daily used by Internet users, as well as technology choices and the evolution of the internet architecture (Arkko et al., 2019).

Technical standards are to be understood as normative specifications enabling systems to communicate with each other, and allowing 'interoperability of different software and hardware' (Cath & Floridi, 2017), whereas protocols consist in 'a set of recommendations and rules that outline specific technical standards' (Galloway, 2004). Both differ from high-level, non-technical standards, such as guidelines on AI ethics and principles, that can be considered at policy level.

1.2. An introduction to standardsetting organisations

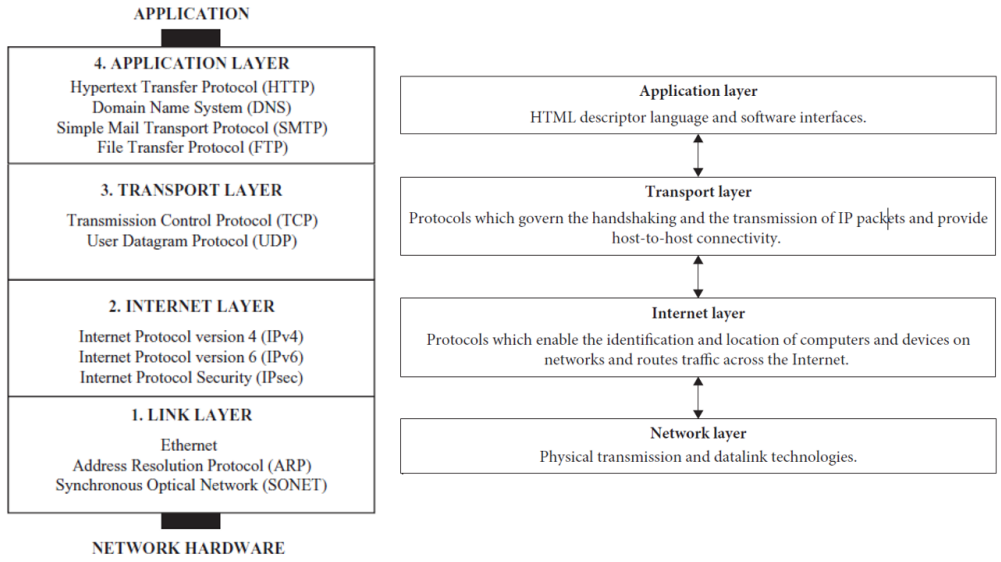
Often overlooked, hundreds of standards and protocols come into play when internet users reach a popular webpage, send an email or watch an online video.

At its most basic, a standard is a normative document describing technical specifications[4]. Standards and protocols are an essential policy instrument in the field of internet governance. Similarly to a legal document, they are written documents containing normative prescriptions. Unlike the law, however, their implementation is usually driven by market dynamics and they often have to rely on voluntary adoption obtained by consensus between experts taking part in their discussion (Rossi, 2021).

The well-known Transmission Control Protocol/Internet Protocol (TCI/IP) model layers illustrate how the different standards comprising the internet can be disaggregated into four layers: network (or link), internet, transport and application (see Figure 1).

[4] The IETF defines standards as 'a specification of a protocol, system behaviour or procedure that has a unique identifier' (RFC 3935, IETF), while the W3C usually refers to the word 'specification' instead of 'standard'.

Figure 1: The traditional TCP/IP protocol suite



Sources : DeNardis (2009) and Harcourt et al. (2020)

Previous works suggest that the system of technological architecture on which the internet relies is not neutral, but can embed values and for instance facilitate (or threaten) the exercise of human rights online (Zalnieriute & Milan, 2019). Though the extent to which it is possible to advance human rights via the internet architecture (Mueller & Badiei, 2019) and 'hard code' rights into protocols (Kiernan & Mueller, 2021) remains subject to debates, it can be argued that the internet standards and protocols directly 'influence the shape of the technically mediated public sphere' (Cath & Floridi, 2017). This is for instance well underlined by the work of the IETF's Human Rights Protocol Considerations Research Group (HRPC), established in 2015.

Internet standards and protocols are notoriously political (DeNardis, 2009) and even more so as digital technologies become pervasive across the world and throughout society. Some of them are 'crucial points of control' over the internet and can serve as a form of public policy (formulated mostly by private organisations), for instance by determining how innovation policy and economic competition can proceed at both national and global levels, or by constituting themselves substantive political issues (DeNardis, 2009). As such, they are an integral part of the mechanisms of internet governance and shaped by a complex web of simultaneous negotiations (Radu, 2019) aimed at improving and transforming the way users, companies and states connect online.

Internet standards are primarily defined by a myriad of understudied standard developing organisations (SDOs) such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Internet Corporation for Assigned Names and Numbers (ICANN), the ITU Telecommunication Standardization Sector (ITU-T), the Organization for the Advancement of Structured Information Standards (OASIS) and the Institute of Electrical and Electronics Engineers (IEEE).

Figure 2: Internet governance-related institutions at regional and global levels

Registries	Intergovernmental fora	EU and national organizations	Key standard-developing organizations (SDOs)
APNIC, ARIN, CENTR, ICANN, LACNIC, RIPE-NCC, national registries (Nominet, Verisign, etc.)	CoE, EU, ePol-NET, ISO, ITU, OECD, UN, WIPO, WTO	CEN, CEPT, ECTRA, ETNO, ENISA, ETSI, NATIA	IAB, IEEE, IETF, Internet Society, IRTF, OASIS, 3GPP, WHATWG, WC3

Source : Harcourt et al. (2020)

Characterised by different genealogies, working processes and membership, these organisations also usually focus on specific technical layers of the internet. For instance, the W3C is an informal body set up by a consortium of universities: the Massachusetts Institute of Technology (MIT) in the United States of America (USA), the European Research Consortium for Informatics and Mathematics in Europe, Keio University in Japan and Beihang University in China. It specialises in developing application-layer standards for the World Wide Web. The Internet Engineering Task Force (IETF), on the other hand, is a private technical standardisation body and has historically been responsible for core internet protocols, such as the original Internet Protocol (IP). It is arguably the most active organisation in internet standards (Harcourt et al., 2020). Unlike the W3C and the IETF, the International Telecommunications Union's Telecommunications Sector (ITU-T) is a UN organisation, thus involving member states, and sets standards mostly at the internet-layer. The Institute of Electrical and Electronics Engineers (IEEE) is a professional body which contributes to the making of key industry standards for the Network-layer, related to Wi-Fi connections, Ethernet or the internet of things (IoT) for instance, and as for the W3C and the IETF, it has no formal state representation. Similarly, the Organization for the Advancement of Structured Information Standards (OASIS) is a non-profit private consortium developing format standards, like the Open Document standard used by OpenOffice and LibreOffice, for the Application layer[5]. The Internet Corporation for Assigned Names and Numbers (ICANN) is another key player in the field of internet governance. It is tasked for instance with the management of IP addresses and of the Domain Name System (DNS). A European non-for-profit entity, the European Telecommunications Standards Institute (ETSI) is one of the three official European standards organisations (ESO) and produces globally-applicable standards for information and communication technologies (ICTs), including mobile, broadcast and internet technologies, mostly at the Network-level.

[5] For more details about the history, governance and characteristics of Internet standards developing organisations, see Harcourt et al. (2020), DeNardis (2009, 2014), Radu (2019), Musiani et al. (2016), Brown (2013) and Mueller (2004, 2010).

Figure 3: Selection of Standards and Standard Development Organisations (SDOs)

Layer	Standards	SDOs
4. Application	XML (data exchange)	W3C, OASIS
	HTTP, HTML (Web)	IETF, W3C
	IMAP, POP, MIME (email)	IETF
3. Transport	TCP, UDP	IETF
2. Internet	IPv4, IPv6, ICMP, ARP	IETF
1. Network	Ethernet, DSL, Wi-Fi, X.25	IEEE
	3G/4G	ETSI

Source : Contreras (2016)

1.3. The politics of standards

These standardising organisations can be seen as a (distributed) field of struggle (Pohle et al., 2016) for companies and states alike, and the locus of influence efforts conducted by powerful actors to defend their political and economic interests through the formulation of technical standards and protocols (Zittrain, 2008). This is well exemplified by recent deliberations within technical standardising networks which have become increasingly subject to the political pressure of governmental authorities, including China (Hoffmann et al., 2020). Recent studies on IETF meetings also reveal that the majority of participants are engineers employed by large technological companies such as Google and Microsoft (Cath & Floridi, 2017; ten Oever, 2020).

The gap between the various interests of stakeholders, but also in terms of their actual power capabilities, is reflected by their diverging visions on what the internet of the future should look like, and in particular whether its fundamental principles[6], and thus core protocols and standards, need to be revisited, or instead forcefully safeguarded. As convincingly argued by DeNardis (2009), these strategies 'reflect competitive struggles for control of the internet and for economic dominance in the internet industry, and reflect how protocols, or even talk about protocols, can bolster and reinforce political objectives'.

Conflicts of interests and agendas in relation to internet standards and protocols are far from limited to the technical discussions of SDOs, as more and more states have expressed their intention to use strategically the making of standards at national or EU levels (Perarnaud, 2021) to leverage influence at the global level. As their objective appears ultimately to 'create an Internet in their own image' (Broeders, 2015), these technical power struggles have thus great implications.

They embody and catalyse significant divergences that have recently fuelled concerns about a growing fragmentation of the internet. Risks and patterns of fragmentation have been observed from the policy side of the internet (Drake et al., 2016) as well as in relation to its infrastructure (Musiani et al., 2016). These academic accounts corroborate observations of a process of 'territorialisation of cyberspace' (Lambach, 2020) and the increasing control of states and large companies over the governance of the internet (Brown, 2013; DeNardis & Hackl, 2015) and in 'ruling its root' (Mueller, 2004, 2010).

[6] These key principles include interoperability, openness, redundancy and the end-to-end arguments (DeNardis, 2014).

2. Methodology

The structure of the report is divided into four parts. The first section provides a typology of patterns of internet fragmentation, presents a number of cases to illustrate their roots and implications and identifies a number of state-based approaches in relation to the making of internet standards and protocols. The second section focuses on the case of the European Union. After a brief history of the role of the EU in internet standardisation, the report explores the implications of current EU legislative proposals for the convergence and divergence of internet standards and protocols. The third section reflects on the main challenges and opportunities for the EU and suggests a number of policy avenues and options to be further explored. Finally, the fourth section proposes a range of policy options and considers their implications in addressing the process of internet fragmentation.

The methodology of the study consists primarily in a comprehensive desk analysis, combined with expert interviews. The literature review covers in particular the recent scholarship in European studies on the making of EU digital policies, social science studies on internet governance and controversies over its infrastructure, the literature in political science and international relations related to power dynamics in standard-setting organisations.

The report also draws on a systematic legal and political analysis of recent EU legislative proposals (including the Digital Services Act, Digital Markets Act, Artificial Intelligence Act, directive NIS 2) as well as non-legislative initiatives (such as the DNS4EU and the Global Gateway initiative). For each dossier, an extensive review of consultation documents, amendments proposals and position papers of all relevant stakeholders has been conducted.

To complement the literature review and validate the findings of the study, twenty interviews were conducted with international experts from different, yet complementary, fields of expertise (policy practitioners, technical experts, and social sciences' scholars). The authors are extremely grateful to Amelia Andersdotter, Sébastien Bachollet, Farzaneh Badii, Stéphane Bortzmeyer, Chris Buckbridge, Alissa Cooper, Ross Creelman, William Drake, Jim Dratwa, David Frautschy, Lise Fuhr, Valentin Grimaud, Alexandra Laffitte, Riccardo Nanni, Mark Nottingham, Niels ten Oever, Maarit Palovirta, Oriane Piquer-Louis, Julia Pohle, Lars Steffen, Adrien Tournier, Peter Van Roste and Rigo Wenning for their contribution to the study.

The study concludes with considerations on various policy options for the EU. Our initial plan was to investigate and assess policy options based on the following method:

- First, we identified proposals made by stakeholders and of amendments made by legislators in ongoing discussions of currently open legislative files was attempted, using methods based on the Advocacy Coalition Framework (Sabatier & Jenkins-Smith 1993) and on the sociology of techno-political controversies (DeNardis, Cogburn, Levinson & Musiani 2020), fed by the collection of a wide variety of policy papers and public statements from a diverse set of stakeholders;
- We conducted our research in a multistakeholder fashion to reflect a diversity of analysis, viewpoints and interests. We conducted interviews with high-level experts from the technical community (e.g IETF and W3C), European businesses in the field of digital technology and civil society;
- Finally, we organised a workshop on Feb. 15th, hosted by the Working Group on Internet Governance and Regulation of the Research Network on Internet, AI and Society (GDR 2091) of the CNRS, with an academic session bringing together internet governance scholars in the morning, and a diverse panel of stakeholders in the afternoon to allow for extensive discussions: potential policy implication, grassroots experience, etc.

This plan had to be adapted due to the fact that internet fragmentation, despite having been addressed by a few reports and been discussed in a number of debates over the years, is still in an early stage of problematisation.

Looking at 62 policy papers and parliamentary reports related to the legislative files we studied, we found that almost all occurrences of the term 'fragmentation' was linked to the fragmentation of the internal market and competition harm, and not to internet fragmentation. We did not find a single occurrence of 'splinternet', 'balkanisation', 'balkanisation' or 'filternet' in these documents, and only two of them used the 'walled garden' expression. Notably, only a few organisations, like CENTR, RIPE-NCC or the Internet Society, that are dealing directly with the technical governance of the internet and the maintenance of its infrastructure, had strong developed statements on the matter of 'fragmentation' as such.

Accordingly, with the exception of experts coming from the technical community running the internet's underlying infrastructure, such as the DNS system, and/or taking part in the technical standardisation of communication protocols, most stakeholders whom we contacted, who took part in the Feb. 15 workshop or agreed to take part in our interviews expressed interest in the topic of fragmentation, agreed that it affected their interests and/or operations, but did not have consistent policy proposals at the ready. In line with conclusions underlined in the first parts of the report, we found that there was not even a shared definition of 'fragmentation' and that most stakeholders were open to discussing the framing of the subject matter. This has led us to adopt a method relying more heavily than originally foreseen on the legal assessment of policy options.

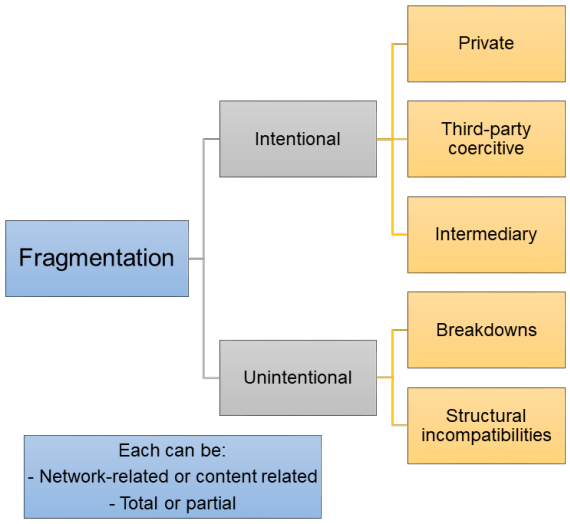
Finally, the study is complemented with three summary lists, in appendices, covering (i) key technologies and protocols under study, and their role in internet divergence and convergence; (ii) key organisations in the development of a selection of internet standards and protocols; and (iii) EU legislative dossiers under study and their relevance to internet fragmentation.

3. Patterns of divergence of internet standards and protocols

The notion of internet fragmentation is a contested topic in the literature on internet governance. A strand of the literature on internet governance argues that internet fragmentation, understood in relation to its technical infrastructure, should not be considered as a major policy issue (Mueller, 2017). Scholars note for instance that the current internet is already composed of thousands of 'islands', known as autonomous systems (AS), which connect altogether 'using interdomain routing protocols and bilateral agreements' (Sharp & Kolkman, 2020). As such, internet is thus fragmented into different systems that remain compatible technically, partly due to network effects (Mueller, 2017). However, this argument is not unanimously accepted. Indeed, another strand of the literature has expressed growing concerns that the internet could be splintering into a 'series of bordered cyberspace segments endangering its very nature' (Drake et al., 2016).

To approach this contested notion, Mueller argues that there are different types of fragmentation which can be either intentional or unintentional (Mueller, 2017), and, according to us, partial or total, network-related or content-related.

Figure 4: Typology of fragmentation processes



Source: adapted from Mueller (2017)

Fragmentation can indeed take different forms, and the assessment of the threat it represents for the internet greatly varies depending on how the internet itself is conceptualised, from a technical infrastructure solely to a global public sphere. This study will conceive the internet more broadly than its material components, and define the internet also in terms of use and local experiences. As convincingly argued by Janet Abbate (2017), the 'limitation of defining the Internet as a large technological system or infrastructure is that this tends to frame the Internet as a channel for transmitting data, rather than as a field of social practice' (Abbate, 2017). Similarly, it will be argued that studies on the fragmentation of the internet should not only consider the technical dimension of splintering processes, but also their commercial, political and social roots and implications. This broad definition will allow us for instance to analyse how the expansion of online profiling techniques has led to practices of ads customisation, and thus forms of individual splintering of the internet.

As the two opposite faces of the same concept, internet fragmentation is directly connected to the state of internet's unity and universality. The more internet is technically fragmented, the less unified it is. Inversely, the greater the internet's universality, the less fragmented it appears to its users. The notion of an 'unified' internet is however far from given, in light of the controversies and power struggles which have constantly re-shaped the internet as we know it.

A short history of the unification of the Internet

The Internet, and the World Wide Web, have provided answers to the problems raised as early as the late 1960s by the Organisation for Economic Co-operation and Development (OECD) regarding the lack of an efficient interoperable and global information system. Although Milton Mueller (2017) has raised the point that network effects now produce economic incentives towards a global, interoperable and open Internet, this has not always been the case. The Internet has had many competitors, and the Web has not always been as smooth an experience of its users as it is today.

In 1978, the French government decided to pull the plug from a research project on a packet-switching network called Cyclades, which was built on the same ideas as what would become the Internet, in favour of Transpac, a network based on the X.25 protocol and not on the TCP/IP suite, which was used by the Minitel. The Minitel, marketed by France's public national telecommunications operator, was revolutionary in the sense that it was the first mass-marketed and widely used product giving access to a digital information network and on-line services. Its success was, however, restricted to the national boundaries of France, and it never led to the creation of the kind of transnational public sphere and marketplace that the Internet is today. It also worked very differently from the current Internet. While the Minitel was a centralised network, where terminals could only be used to access content, and never host it, the Internet was built as an 'end-to-end' network in which the network only transports data packets, and where all end nodes can be either clients, servers or both (Musiani & Schafer, 2011).

Beginning in 1977, the International Organisation for Standardisation (ISO) launched a wide effort, supported by states and by the International Telecommunication Union (ITU) to define a new network architecture, called Open Systems Interconnection (OSI). At the time, the proposed TCP/IP protocol suite on which the Internet now runs was seen as one among many other experimental protocols that were supposed to progressively fade away once OSI would have been implemented. Its governance structure was radically different from the multi-stakeholder, often informal processes of Internet governance, and was met by strong resistance by supporters of the latter (Russell, 2006).

Other competitors emerged from the private market. Until the mid-1990's, the Internet was mostly used for non-profit purposes, and essentially academic and military ones. Arpanet and the National Science Foundation Network (NSFNET), its main networks, did not allow commercial use. UUCPNET, which used Unix-to-Unix CoPy software, did not have such restrictions, and allowed commercial use, but was theoretically banned from interconnecting to Arpanet and NSFNET. Some private companies had also started offering private on-line services since the end of the 1970s. Before offering Internet connectivity in 1989, CompuServe, for example, had maintained its own proprietary network to provide its online services (Bing, 2009).

When, in the early 1990s, the restrictions on the commercial use of the Internet were finally dropped, this created difficulties for private, non-interoperable commercial on-line services. As telecommunication networks were progressively liberalised, consumer demand turned towards the global Internet. A turning point was in 1995, when one year after having launched its own proprietary on-line service called MS Net, Microsoft abandoned the project (Rebillard, 2012).

Even once Internet protocols had prevailed over competing initiatives and TCP/IP became the established standard for computer networking, and the Web, invented around 1990 by Robert Cailleau and Tim Berners-Lee at the European Organization for Nuclear Research (CERN), overtook Gopher as the standard for accessing on-line content because the university that licensed it refused to pledge to provide it royalty-free (Russell, 2003), fragmentation still remained due to what has been called the 'browser wars'. Indeed, despite attempts made by the World Wide Web Consortium, established in 1994, to impose a common version of the web's core languages, HTML (HyperText

Markup Language) and CSS (Cascading StyleSheets), accepted on all devices and all web browsers, the fierce competition between the two market leaders of the late 1990's, Netscape's Navigator and Microsoft's Internet Explorer, led to divergent implementations that broke interoperability. For users, this meant that the appearance and even the availability of web content would depend on the software they were using. By being the first to introduce frames and coloured backgrounds in their free browser, and being the biggest player in the browser market, Netscape ensured that publishers would pay the $50.000 price tag for their web server software and not go to the competition (Windrum 2004).

However, by leveraging the quasi-monopolistic market share it had in the consumer operating system market, Microsoft managed to impose Internet Explorer as a near-hegemonic market leader. While Netscape owned 90% of the market in 1995, its user base had dwindled to a mere 23% by 1999, against Microsoft Internet Explorer's 76% (Windrum, 2000). In a couple of years' time, Internet Explorer had thus become hegemonic. This was challenged by the Department of Justice in the United States in a lawsuit, which led to a settlement in which Microsoft agreed to share its application programming interfaces (APIs) with other companies. In 2009, the same company, under the pressure of the European Commission, agreed to present Windows users a choice on the browser they want to use, instead of tying Internet Explorer with the operating system. The arrival of new actors, such as Mozilla, Apple and Google, created renewed competition in the sector of web browsers and gave more power to the W3C to broker interoperable and open standards, making websites more reliable and the web experience more unified across devices.

In 1997, an alliance of actors of the mobile phone industry set up the WAP Forum to standardise the Wireless Application Protocol (WAP), keeping their distances with Internet governance institutions like the Internet Engineering Task Force. This, in effect, created a parallel hypertextual environment, separate from the Web, as the Wireless Markup Language was not interoperable with HTML (Kumar, Parimi & Agrawal, 2003). However, the WAP protocol, which had been set up mainly due to the technical limitations of mobile phones in the 1990's, has now been long abandoned in favour of web standards provided by the W3C.

Legislation on limited liability for intermediaries and net neutrality drawn up several legislations across the world, and in the European Union also had, for some of it, effects that strengthened a unified Internet. The e-Commerce Directive (Directive 2002/31/EC), by excluding service providers that modify the information that is transmitted from the limitation of liability provided by its articles 12 for mere conduits and 13 for caching services, strengthens the Internet's end-to-end principle. Finally, Regulation 2015/2120 laid down rules to protect an open Internet and network neutrality, meaning that network actors may not refuse or alter connectivity to any other lawful actor.

Taking into account the long history of the project of building an open and unified internet, this study investigates the convergence and divergence of internet standards and protocols in relation to the existing threats to internet's unity and openness. In his 2017 book *Will the Internet fragment? Sovereignty, Globalization and Cyberspace*, Milton Mueller proposes an innovative taxonomy to map the main threats to the unity of the internet. Adding a range of new threats and cases to the original taxonomy, this study will use this framework to approach the many different factors leading to the apparent divergence of internet standards and protocols, as well as their implications.

The taxonomy of threats initially developed by Mueller (2017) differentiates between threats related to technological factors and threats linked to social and political factors. In this context, technological factors include (planned) obsolescence, internet outages, the division of the DNS root, incompatible protocols, Network Address Translation, application-layer incompatibilities, the absence of device and net neutrality, data localisation practices and content filtering. As for the social and political factors, they refer for instance to the consolidation of the internet with the rise of the platform economy as well as the 'internet's alignment' with national interests and legislations. Drawing on this framework of analysis, the report will underline a number of key current threats for internet's unity, and will later highlight their relevance and how they can be addressed in the EU context.

3.1. Technological factors

This section explores the scope of technical factors which can be considered as threats to the unity and openness of the internet. Indeed, a number of technical protocols and standards are directly relevant to the study of internet fragmentation. Though the process of their formulation and deployment is often strictly beyond the realm of the European Union's competences and capabilities, the following cases highlight why it is necessary to study these developments, identify their relevance to EU digital policies, and propose avenues to address these challenges.

From a technological perspective, a number of threats to internet's unity can indeed be identified. Many directly derive from the lack of interoperability. When technical protocols become incompatible, they risk creating independent silos in the network. This applies also to the other end of the internet stacks, with incompatibilities in the application-layer. Meanwhile, the intentional (or unintentional) obsolescence of protocols, devices or applications can further fragment connectivity on a global scale. These threats will be illustrated through the following cases.

3.1.1. Network address translation: From IPv4 to IPv6

Among the many contentious issues related to internet protocols, the limitations of the internet Protocol version 4 (IPv4) appears as one of the most long-standing. It relates to one of the most essential resources for the functioning of the internet, namely Internet Protocol addresses.

The accelerating growth of the internet led to a growing awareness about the limited stock of IP addresses provided by IPv4, and the constraints it could pose for businesses and public organisations alike. This constraint fuelled the practice of investing in Network Address Translations (NAT) systems. Instead of relying on (limited) public IP addresses, NAT allows organisations or ISPs to create private numbering networks for local use. To connect with the public internet, these private addresses are then translated into public addresses using NAT systems. As argued by Drake et al. (2016), this process introduces 'the possibility of a kind of fragmentation in the internet because the private addresses are isolated from the rest of the Internet unless they pass through a so-called NAT box (that could be part of a router)' (Drake et al., 2016).

In order to address the exhaustion of the number of internet addresses that could be allocated under the IPv4, the internet community, and more specifically the IETF, developed a new standard known as IPv6 in the years 1990s. The ground-breaking book *Protocol Politics* (2009) of Laura DeNardis carefully documents the context in which this new internet protocol emerged and the contentious processes leading to its design and (limited) initial deployment.

One of its main added values is to greatly expand IP's addressing capabilities. Indeed, IPv6 increases the IP address size from 32 bits to 128 bits, and thus augments the number of IP addresses from 4 billion to approximately 340 undecillion (or 2^128) addresses. Though it has been the subject of intense debates, IPv6 also intended to improve data integrity and privacy for end users[7]. The design of IPv6 protocols eventually led to the adoption of an IETF Draft Standard in 1998[8].

Faced with the increasing scarcity of IPv4 addresses, but also with the promising prospect of investing early in a technology not yet dominated by US interests and companies, the EU and many national governments (Japan and China for instance) launched strategies in order to accelerate IPv6

[7] DeNardis (2009) indeed recalls the concerns expressed by the EU Article 29 Data Protection Working Party and the formal response that had been published by the European Commission's IPv6 Task Force at a time. One of the main issues revolved around the possibility opened up by IPv6 to track mobile users based on the unique identifier embedded in their IP address.

[8] In 2017, following the process of IPv6 maintenance, the IPv6 protocol became officially an Internet Standard of the IETF (RFC8200).

deployment. DeNardis (2009) explains how IPv6 did not spark an equivalent rush in the United States, partly due to the vast reservoirs of IPv4 addresses held US actors. This situation evolved in the years of 2000s after the US military identified that such transition would strengthen cybersecurity but also help to support new military applications, which led to a directive of the Department of Defense mandating a transition to IPv6 by 2008.

Rather than an orderly migration from IPv4 towards IPv6 as initially expected twenty years ago, scholars have observed a form of 'standards competition' opposing IPv4 and IPv6, caused primarily by their incompatibility but also diverging economic incentives (Kuerbis & Mueller, 2020). Indeed, a device exclusively using IPv6 is not able to directly exchange data with a device exclusively using IPv4. If not addressed, such incompatibility could significantly affect Internet users' experience by preventing their access to a webpage or hindering their communications online.

The prominence of IPv4 across the world and the additional costs required for maintaining a compatibility with IPv6 have significantly hindered the deployment of its successor. Most upgrades by companies and operators involve dual protocol stack implementations using both protocols. Even in the case of large cloud providers, actors known for their relatively high deployment of IPv6, Kuerbis & Mueller (2020) indicate that many have 'built IPv6-enabled services to become qualified for U.S. government contracts, but the majority of their revenue is derived from services delivered over IPv4 connections'.

As a result, the success likelihood of the replacement of IPv4 by IPv6 as the main network layer protocol has become very much debated in the literature (Levin & Schmidt, 2014; Dell, 2018). The possibility of a splintering of portions of the internet, relying exclusively either on IPv4 or IPv6, remains however as unlikely. Still, this means that the permanence of NAT and private numbering plans will remain a threat to internet's unity for the near future.

This situation underlines how the adoption and implementation phases of standards can be as important as their formulation. The various attempts by national governments and the EU to use the IPv6 upgrade as a strategic tool to leverage political and economic influence in the years 2000s clearly demonstrate how technical protocols can become instruments of power and their deployment an opportunity to challenge the dominance of (in this case US-based) commercial competitors. The case of IPv6 also underlines how technical protocols have the capacity to greatly transform the architecture of the internet, but also to re-define its usage and the possibilities it offers. For instance, the widespread deployment of the internet of things (IoT) is expected to heavily rely on the capabilities offered by IPv6 protocols (Minoli, 2013).

The development of private addressing systems and the contentious politics behind the deployment of IPv6 show the challenges posed by the lack of compatibility of technical protocols for internet's unity and openness. The following examples looks at other important layers of the internet stacks, uncovering instances of competition and incompatibilities at the transport and application layers.

3.1.2. Protocol competition at the transport-layer: The development of TLS 1.3 and ETS

TLS is the most widely known and used security protocol for implementing cryptography on the internet. It was first specified in 1999 (TLS 1.0), as the successor and improved version of Secure Sockets Layer (SSL), originally developed by Netscape Communications Corporation. This protocol uses a combination of cryptographic tools to provide communications security for client/servers applications.

In twenty years, the TLS protocol has evolved into the Transport Layer Security version 1.3 (IETF, 2018), which became a formal standard of the IETF in 2018. The development of TLS 1.3 was accelerated by the Snowden revelations in 2013, and the growing intention of the technical

community to make encryption the norm for internet traffic in light of the vulnerabilities of TLS 1.2. One of the documents disclosed by Edward Snowden indeed showed that the US National Security Agency (NSA) had pushed for the introduction of a cryptographically weak random number generator allowing for the possibility to decrypt encrypted communications passing through the internet architecture.

The development of the TLS 1.3 was carried out by IETF's TLS working group. Harcourt et al. (2020) suggest that engineers from large internet companies, such as Google, Apple, Facebook and Microsoft, were the main authors during the design of the protocol. Kiernan & Mueller (2021) also note the active participation of Cloudflare and contributions from the NSA and civil society organisations in the development phase. One of its main improvements is the strengthening of so-called 'forward secrecy', which mandates the use of a unique and random ephemeral encryption key for each network session (based on the Ephemeral Diffie-Hellman key exchange protocol). Previous versions of the TLS protocol indeed gave eavesdroppers the possibility to decode previous sessions once a server's private key was found.

Despite contestation within IETF, and in particular from network operators and the banking industry (Kiernan & Mueller, 2021), the protocol TLS 1.3 was agreed in 2018. As argued by Harcourt et al. (2020), the main issue has become its actual implementation, notably by the companies and states initially opposed to the introduction of ephemeral cryptographic keys for various economic and security reasons.

Kiernan & Mueller (2021) indeed show how a number of actors (including US governmental agencies and financial institutions in particular), which were unsuccessful in pushing for the status quo (maintaining static private encryption keys), decided in 2017 to lead the charge in another standardising body (ETSI) to develop an alternative transport protocol.

As a result of this effort, ETSI's technical committee on cybersecurity recently created the new transport protocol known as Enterprise Transport Security (ETS), which relies on static encryption keys[9]. The competing implementation of both protocols is ongoing and is expected to play a crucial role for the security of online communications globally for the coming years (Hoffman-Andrews, 2019).

This current competition between TLS 1.3 and ETS could thus give rise to a new form of divergence for internet users, in terms of the level of security provided when using the internet.

These cases underline the challenges brought by technical incompatibilities and divergences for the internet's unity and openness. They only provide a snapshot of existing technical challenges, as other cases would deserve a closer examination. In a fourth instance of technical factors underlying forms of fragmentation and/or divergences of standards, the following section looks at the DNS and challenges raised by Internationalised Domain Names (IDNs).

3.1.3. The lack of universal acceptance for internationalised domain names

IDNs allow for the registration of domain names in local languages and scripts, using non-Latin characters (including Arabic, Hindi, Chinese or Cyrillic). The promotion of IDNs and the development of a multilingual internet have been a constant feature of internet governance debates over the past decades (Bygrave et al., 2009). The lack of a multilingual feature of the DNS was already identified as an important issue in the 1990s, as internet domain names were seen as 'limited to a very restricted character set' (Duerst, 1996). Originally, the DNS was originally restricted to American Standard Code

[9] For more, see: https://www.etsi.org/deliver/etsi_ts/103500_103599/10352303/01.01.01_60/ts_10352303v010101p.pdf.

for Information Interchange (ASCII) characters, thus precluding the possibility of domain names in other language scripts (Musiani, 2013).

The implementation of IDNs began in 2000 for second-level domains (IDN World Report, 2019). Following these developments, the IETF launched a new Working Group for Internationalised Domain Names (IDN) in 2008 to refine requirements and establish new standards for the use of non-Latin characters in domain names, by introducing changes to the already existing IETF's 'internationalising domain names in applications' (IDNA) standard. Then, in 2010, the implementation of country code top-level domains (ccTLDs) for native language scripts became a reality.

However, the deployment and implementation of IDNs have been hindered by a variety of challenges, some of them related to cybersecurity, but also technical difficulties. This appears directly connected with the issue of internet fragmentation since the lack of IDNs prevents a significant portion of the world population to access the internet using their own language, while technical errors and the lack of universal acceptance further complicate the use of IDNs. In 2021, approximately 2.5% of all domain names were IDNs according to the IDN World Report[10].

From a technical standpoint, the deployment of IDNs is hindered by the lack of a uniform processing of domain names written in local scripts, at different nodes of internet stacks, which ultimately result in repeated technical errors for internet users accessing domain names in local languages. Also, internet users with an email address in a native language script may have difficulties to communicate, or may fail to have their address recognised when registering on an online platform. The barriers to uptake for IDNs are thus manifold. They include the lack of email compatibility as well as limited internet browser support for using IDNs. For instance, a recent study conducted by the ICANN's Universal Acceptance Steering Group showed that among a selection of popular websites only 8% of them authorised for the use of internationalised email addresses.

Yet, technical factors are far from being the main drivers of the process of internet fragmentation and divergences of internet standards. The following section identifies a number of cases related to market and commercial developments.

3.2. Commercial factors

As already illustrated by the previous cases, technological companies can be important drivers or catalysers of internet fragmentation, as their commercial interests may enter in conflict with the goal of ensuring the unity and openness of the internet. Indeed, certain corporate actors, and notably Google, appear on their way to shape an independent technical infrastructure, which could be conceptualised as end-to-end, by building their own undersea cables and data centres, developing their own protocols and directly providing data and services to end-users.

This concentration of power, knowledge and wealth has given a considerable pre-eminence to a few large companies and states in the fora discussing the making of the standards and protocols of the internet of the future. As argued by Weyrauch & Winzen (2021), this suggests that 'the internet fosters the concentration of authority, market shares, and other characteristics such as centrality in standards development in a few major companies'. Though participation is usually open to any interested party, the main participants to standards developing organisations indeed come from the United States and Western Europe (Harcourt et al. 2020). However, Hoffmann et al. (2020) observe that the 'participation of delegations of governments from Western countries has

[10] The IDN World Report is a collaborative effort between EURid (the .eu Registry), UNESCO, and the Coordination Center for TLD.RU.

decreased. Such governments prefer industry-led, market-driven standards which reflect the demand for standards from the companies and organisations who use them'.

Private internet SDOs are for a large part made up individuals working for the private industry and who effectively carry out most internet governance decisions, such as designing protocols (DeNardis, 2009). Historically, these organisations have been set up to foster an open and universal internet. This has been recently reaffirmed by a statement by the *Ethical Web Principles* drawn up by the Technical Architecture Group of the W3C, which first article states that:

> *There is one web*
>
> *When we are adding new web technologies and platforms, we will build them to cross regional and national boundaries. People in one location should be able to view web pages from anywhere that is connected to the web.*
>
> Source: Appelquist and Beeman (2020).

Large internet and telecommunications companies are thus important drivers in the formulation of internet protocols. Though many actors benefit from open standards, it could be argued that the 'increasing control over internet infrastructure and services by a small set of organizations' (Arkko, 2020), now often described as the process of 'internet consolidation' (Taylor & Hakmeh, 2020), may appear as a greater threat to the internet than existing conflicts surrounding protocols and standards themselves. Hegemonic actors may be tempted to forego formal standardisation processes, which require time-consuming consensus and, more importantly perhaps in key standards-setting fora, to pledge royalty-free access to essential intellectual-property-related claims related to the standard being agreed upon (Russell, 2003). At times, market actors with significant weight may be tempted to impose their decisions unilaterally. In 2017, Apple, a key player in the mobile browser market, decided to drop support for Adobe Flash in 2010 (Jobs, 2010), precipitating the end of this proprietary technology. More recently, it decided to block all support and connectivity for Point-to-Point Tunneling Protocol (PPTP), one of the protocols used to establish VPN connections (Apple, 2018). Similarly, as we shall see, Google has used its weight to impose the QUIC protocol and its privacy approach in the case of the Federated Learning of Cohorts (FLoC). These decisions may create patterns of fragmentation from the end user's perspective.

It should also be emphasised that 'standards wars' between corporate actors (Kuerbis & Mueller, 2020) are not only waged during the phase of their design, but are also fought as part of their implementation and adoption (Kiernan & Mueller, 2021). Simcoe & Watson (2019) convincingly show how large technological companies may be incentivised to support the design and adoption of open standards, to then 'fork' them by adding proprietary extensions that competitors may not implement, in view to extinguish the competition and the original open standard.

The following cases illustrate the commercial factors and patterns that may represent challenges for the unity of the internet, starting at the transport-layer with the development of QUIC and the concentration of the DNS resolver market, followed at the application layer by insights provided by the recent release of FLoC by Google.

3.2.1. The case of the deployment of Quick UDP internet connections (QUIC)

In the context of standard-developing organisations such as the IETF, states and large companies compete to define the standards of the internet of the future (Mueller, 2017). The recent deployment (and success) of the new transport protocol QUIC in Google's browsers and web servers is indicative of the struggles and capabilities deployed by these actors. After being released by Google in 2013, more than three quarters of Facebook's traffic is now already over HTTP/3 and QUIC (Facebook, 2020).

QUIC (Quick UDP internet connections) is a transport layer network protocol first designed by Google, and notably by one of its engineers Jim Roskind. QUIC was first presented at the IETF in 2013. The IETF QUIC working group was launched a few years later (in 2016) in view to standardize this protocol, which became an IETF standard in June 2021. The main objectives of QUIC are to lower latency and improve performance and security of transport protocols. Instead of TCP (Transmission Control Protocol), QUIC works on top of UDP (User Datagram Protocol), a core Internet protocol known for its 'simpler' connectionless communication model[11].

Google is considered as the primary initiator in the design and rolling out phases of this standard. The company designed this protocol (known as G-QUIC) for its own services, and then identified strong incentives to proceed to its standardisation at the global level via IETF. Harcourt et al. (2020) argue that Google's motivations were commercial, regulatory, but also technical (in resolving the latency and 'ossification' of TCP). It is enabled by default on Google Chrome and used by other services of Google such as YouTube. Other companies including Microsoft, Cloudflare, Ericsson, Akamai and Facebook have announced their intention to deploy QUIC at scale in 2021 (IETF, 2021b).

Interestingly, the new HTTP/3 has been built on top of QUIC, rather than TCP. This constitutes the first instance of an application designed to run over QUIC. From 5% in February 2021, HTTP/3 is now used by more than 20 % of all the websites as of August 2021[12]. This exponential growth corroborates a statement from the CTO of F5, a large technological company, that QUIC will soon 'eat the Internet' (Duke, 2021). The ongoing deployment of QUIC across some of the largest internet platforms underlines the ability of Google to propose and advocate for protocols in line with its own economic and technical imperatives. Indeed, limited latency in the access to websites had been identified as a highly profitable opportunity, given the observed effect of latency on websites' revenues.

It is important to note that the standardisation process of QUIC at the IETF was carried out in conjunction with the one of TLS 1.3. Both standards streams had as common goal to improve the security and privacy of communications. QUIC indeed encrypts almost all of transport information, mainly at the expanse of network operators. In terms of security, one of the implications of the parallel roll-out of QUIC and HTTP/3 is indeed that traffic analysis has become much more difficult for network operators, and requires the development of security solution at an application-level (Drake, 2021). This shift favours certain operators, such as Google, which can provide these services. Though not a direct threat to internet openness, the ongoing deployment of QUIC is an interesting instance of how protocols can foster forms of internet consolidation. Yet, it needs also to be recognised that QUIC, in the context of HTTP/3, is a protocol that could also improve the quality of global connectivity, and thus help address existing divides between internet users across the world.

The following case focuses on another understudied transport-related protocol – DNS name resolution – to show the implications of patterns of internet consolidation for its unity and openness.

3.2.2. The concentration of the DNS resolver market

DNS resolvers are servers with the function of converting domain names into IP addresses. Traditionally carried out by ISPs, this function has been increasingly given to emerging actors, proposing more efficient and tailored results (for instance through censorship) than ISPs.

Radu & Hausding (2020) shows how the domain name system (DNS) resolver market is subject to patterns of consolidation. This technical arena, which is essential for the functioning of cloud services and content delivery, is indeed increasingly characterised by processes of concentration with significant economic and political implications. Evidencing this pattern, the study of Hoffmann

[11] For more, see: https://peering.google.com/#/learn-more/quic.

[12] For more, see: https://w3techs.com/technologies/details/ce-http3.

(2019) shows that less than ten companies currently resolve half of the global internet traffic, with Google having the strongest position with its Public DNS. Recent data from APNIC Labs[13] validates that in the DNS provider environment, Google is the dominant provider across the entire internet (Huston, 2019), while other providers appear to be used at a more regional level (in China and Russia in particular). Interestingly, DNS resolver services are usually free of charge, but remain profitable in light of the precious intelligence they offer to the few technological companies providing this service.

Moreover, Radu & Hausding (2020) also note that 'global service providers of public DNS resolution services are not restricted in their practices by regulatory provisions, national control points or self-imposed codes of conduct and might respond to internal and external pressures in unpredictable ways'. This is well illustrated by the recent development of two DNS protocol extensions, DNS over TLS (DoT), standardised in 2016 following the Snowden disclosure, and DNS over HTTP (DoH), introduced by Google and standardised in 2018. With web browsers increasingly implementing these protocols, ISPs' role appears more and more limited in comparison to mostly US-based resolvers.

The growing concentration of DNS resolution services has a direct impact for internet openness and unity, given the repercussions it has in redistributing the power between key actors (particularly network operators and internet companies), as well as in the capabilities and leverages it provides to a few corporate actors in resolving all the internet traffic.

From these cases, it appears that internet services and technological companies have a significant role in the acceleration of patterns of consolidation and 'splintering'. Within the same legal jurisdiction, divergences in the internet access of users can also derive from 'demand-side' customisation. This indeed determines how the same broad internet content can be filtered and delivered to different users. The following case investigates this phenomenon by unpacking the implications of the recent release of FLoC by Google.

[13] Updated data on the use of DNS resolvers in the world can be found at: https://stats.labs.apnic.net/rvrs.

3.2.3. Ad-based profiling and the FLoC proposal

The expansion of internet users' profiling techniques has led to the generalisation of practices of customisation, and thus forms of individual splintering of the internet. While such divergences may be described as different views of the same internet, their cumulative effect can be substantial. This is partly due to the increasing sophistication of the profiling techniques developed by the ad tech market.

Most segments of the display advertising ecosystem are controlled largely by Google. Indeed, its dominance over the ad tech market (including via 'programmatic advertising' or real-time bidding, RTB) has led to concerns that this company may engage in 'both exploitative and exclusionary strategies' through vertical foreclosure (Geradin & Katsifis, 2019).

This is well exemplified by the recent controversy over the release of FLoC (for Federated Learning of Cohorts) by Google, as part of its new Privacy Sandbox. This initiative, launched by Chrome in 2019, developed new application programming interfaces (API) to improve the privacy of its technologies 'while supporting a thriving ad-funded web'. This project has been abandoned by Google officially in January 2022, and replaced by the new 'Topics API'[14], which introduces a similar system of interest-based advertising.

The main idea behind FLoC was to replace advertisings based on individual identifiers and thus individual cross-site tracking by third parties. Such tracking is usually implemented through third-party cookies to track users' browsing behaviour across multiple websites. In order to replace third party cookie-based advertising, FLoC instead intended to cluster groups of people with similar browsing habits. FLoC relied on a machine learning system which tracks browsers habits via the web browser Chrome, and groups together users into so-called 'cohorts' labelled with a group identifier[15]. The classification of users into specific categories was done locally (at the browser level) and did not require a central server that could centralize personal information (Langheinrich, 2021). Users shared this code in their interactions on the web, and ad tech companies could use it to target specific cohorts. By doing so, Google claimed that it would 'fundamentally enhance privacy on the web' by creating an 'ad-supported web in a way that will render third-party cookies obsolete' (Schuh, 2020)[16].

This proposal also introduced a profound change in the way ad tech actors would operate by transforming web browsers 'into the sole entity able to track users across sites and assign them to cohort' (Geradin et al., 2021). FLoC was thus expected to have great implications for ad tech vendors. The phasing-out of third party cookies means that they would increasingly rely on web browsers which will effectively become the gatekeepers of the advertising ecosystem. FLoC indeed built on Google's large-scale infrastructural control and coordination, provided by the dominance of its web browser Chrome and its capacity to orchestrate a protocol through it (Veale & Zuiderveen Borgesius, 2021).

Critics of the proposal have pointed out how Google 'leaves intact the ability of a publisher to track users on the basis of a first-party relationship' and 'will do nothing to limit tracking undertaken on the major platforms operated by Google and Facebook' (Geradin et al., 2021). As a result, this proposal nourished concerns of market concentration. A recent report by the United Kingdom's Competition and Markets Authority (CMA) argues that these changes would further reinforce Google's position in the online advertising market given 'its ability and incentives to exploit the intermediation chain to self-preference its own activities' (CMA, 2020). In addition, the European

[14] For more, see: https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/.

[15] Google claims it will never create cohorts with less than several thousand users.

[16] EFF instead argues that it will provide highly sensitive information to third parties, and as such does not protect privacy (Cyphers, 2019).

Commission announced in June 2021 a formal investigation into possible anticompetitive conduct by Google in the online advertising technology sector, which intends to address the future prohibition of third party 'cookies' on Chrome[17].

Before its official replacement by 'Topics API', which relies on a similar system, FLoC had been under a phase of testing, and was implemented with a small percentage of users in Australia, Brazil, Canada, India, Indonesia, Japan, Mexico, New Zealand, Philippines and the United-States (Vale, 2021). Following the launch of a formal investigation into the Privacy Sandbox by the United Kingdom's CMA in January 2021, Google announced new commitments in relation to the phasing-out of third party cookies and also postponed its full implementation. Google for instance ensured that it 'will not build alternate identifiers to track individuals as they browse across the web', nor use these identifiers in its products. Google stated that it 'will not give preferential treatment or advantage to Google's advertising products or to Google's own sites' in the context of its Privacy Sandbox (Bethell, 2021). Similar concerns are now being voiced in the context of the 'Topics API' proposal. It can be argued that given their consequences for the ad tech business model, these changes have a direct impact on existing forms of individual splintering, and are likely to re-shape significantly internet's usage and users' online experience in the near future.

The following example turns to the functioning of web browsers and explores the under-studied case of Blink, the browser engine recently developed by Google.

3.2.4. Incompatibilities at the application-layer: the case of web browsers' engines

Recent allegations of YouTube' slowing down with Firefox browsers have recently fuelled concerns of intentional incompatibilities introduced by Google to disadvantage its competitors in the web browsers market. Indeed, the loading of YouTube on Firefox became slower after Google redesigned YouTube's interface based on an update only implemented in its own web browser Chrome (Keane, 2018).

This case underlines the threat posed by incompatibilities at the application-layer as they can become conducive for more internet fragmentation. When, intentionally or not, languages and lay out engines used by web pages and applications cannot easily connect among themselves, this has a direct impact on internet's usage and users' experience. Further exploring the recent allegations of YouTube' slowing down with Firefox browsers, the following section will see how a core component of web browsers' program, their browser engine (also called rendering engine), can directly participate to internet fragmentation.

The main role of a browser engine is to collect various types of codes (such as HTML) on webpages and translate them into the final visualisation on the display screen for the end user. Web browsers Google Chrome and Opera have been using Blink[18] since 2013. Blink is an open source browser engine part of the Chromium project. Though developed with contributions from Facebook, Opera, Adobe or Samsung, its main and largest contributor has been Google. After attempts to use alternative solutions, including EdgeHTML, Microsoft opted for Blink as well for its own browser in 2019. This choice was partly justified by the difficulty of Microsoft to develop EdgeHTML and make it compatible for Google's websites such as YouTube.

Harcourt et al. (2020) indicate that Google Chrome 'is currently demonstrating increasing divergence' towards agreements in SDOs (such as the W3C) in an attempt to disrupt competing web browsers. In this context, the compatibility of various websites with web browsers has thus been

[17] For more, see: DG COMP, Case 40670 'Google - Adtech and Data-related practices', 22.06.2021. URL: https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40670.

[18] See 'Blink (Rendering Engine)', The Chromium Project (Web Page). URL: www.chromium.org/blink.

leveraged as a way to advantage particular platforms over others. This partly explains why the largest web browsers – Chrome, Opera, Brave, Yandex and Edge – use Blink. Mozilla Firefox stands out with its own open source browser engine Gecko, while Apple's browser Safari uses WebKit derived from the KDE Project's KHTML (and the basis of Blink) as browser engine.

This situation has led scholars and experts to worry about the re-emergence of the era in which Internet Explorer exerted a quasi-monopoly in the market of web browsers in the beginning of the years 2000s, which was characterised by anti-competitive practices and the depreciation of alternative browsers. At a time, Internet Explorer gathered more than four fifths of the web browser market and 'Microsoft's strategy was increasingly characterised as an effort to 'embrace, extend and extinguish' a set of standards that might threaten the dominance of its Windows platform' (Simcoe & Watson, 2019). For instance, Mark Nottingham, co-chair of the IETF's HTTP and QUIC Working Groups, argues that 'if Google had never forked WebKit to create Blink and then Chrome, it is likely that the remaining browsers at the time – Firefox, Safari, and Internet Explorer (now Edge) – would still have significant market share, to varying degrees' (Notthingham, 2021).

The little-known case of Blink clearly exemplifies the negative effect of incompatibilities at the application-layer for the internet's unity and openness. It shows how technical components can be used as strategic tools by technological companies to control digital markets, and participate to the shaping of a less interoperable and more fragmented internet. Indirectly, these incompatibilities can also lead to the planned obsolescence of protocols, devices or applications, and thus foster even more fragmentation.

While these programs and protocols are rather technical, they are of significant importance because they provide concrete means for shaping future internet landscapes. This is particularly relevant for emerging technologies such as artificial intelligence, 5G/6G and the internet of things (IoT). This section emphasised that one of the main challenges in this context relates to an increasing organisational concentration within standard-making bodies, in light of the predominant role played by internet monopolies in these fora.

This review can only identify a limited set of developments to illustrate the role of commercial factors in reinforcing patterns of fragmentation. At a more general level, other developments would deserve closer attention, such as the broader process of 'platformisation' of the internet (Poell et al., 2019), and the rise of 'zero-rating' practices, as shown recently by the case of Facebook's *Free Basics*. Zero-rating can be defined as the practice, implemented by various ISPs and telecom operators, to provide internet access with no direct financial cost for consumers when accessing specific websites and platforms (such as Facebook). As argued by Belli (2016), due to these trends 'users are actively disincentivised from venturing beyond the zero-rated applications and steered into a Minitel-like environment, thus fostering fragmentation of the internet into subsets of services predefined in a top-down fashion by single operator'. These broader developments are also important drivers of internet fragmentation as they foster the fragmentation of the virtual space from the perspective of internet users.

In the next part, after having underlined the great power of large technological companies in the making process of core components of the internet stacks, the crucial role of states is to be highlighted.

3.3. Political factors

In addition to the previous interrelated technical and commercial factors constituting threats to internet's unity and openness, the role of states and their strategic interests to exercise power in and through cyberspace (Deibert & Crete-Nishihata, 2012) need to be recognised as instrumental, and to some extent primary, drivers of internet fragmentation.

3.3.1. The internet's increasing alignment with territorial borders

Global state powers such as Russia, the USA, the EU and China are increasingly taking strategic approaches towards internet standards, in an effort to 'recreate the power structures of national governments in cyberspace' (Mueller, 2017). As already evidenced in the previous sections, states develop their strategy through the work of their administration and public representatives, but also by leveraging their control over (national) companies and academia. This suggests that increasingly 'geopolitics infects the internet's deep technical layers' (Hoffmann et al., 2020). Though SDOs appear dominated by companies and the technical community, states have important tools to influence their decision-making. Harcourt et al. (2020) mention for instance how the decision of SDOs such as the W3C or the IETF are 'permissible under international and national agreements and agencies'. This applies in particular in relation to intellectual property and standardisation (Lundqvist, 2014). For states, technical standard can become a source of strategic and commercial advantage, give legitimacy to national regulatory efforts aimed at digital technologies, and project alternative ideas for the internet infrastructure (Hoffmann et al., 2020).

Instead of internet fragmentation, Milton Mueller (2017b) has proposed to qualify this pattern of partition of the cyberspace along geopolitical borders as 'alignment'. Internet alignment can be fuelled by 'efforts to filter content to make it conform to local laws; to require companies to store their users' data in local jurisdictions; to keep internet routing within state borders; to require governments or users to rely on local companies rather than foreign ones for equipment and services; to link cybersecurity to national security' (Mueller, 2017b). Driven by a number of economic, political and strategic factors, the development of national firewalls to control internet traffic and increasing attempts to build 'sovereign' internet infrastructures, coupled with the introduction of data localisation requirements as well as new obligations for internet service providers at national level, can indeed have a significant impact for the openness and unity of the internet. The increasing number of intentional internet shutdowns ordered by national authorities across the world is another visible trend illustrating this process of partition. These practices are further exemplified in the following section, looking at specific state approaches.

Before addressing the role and action of the EU in relation to safeguarding the internet's unity and openness, this section will explore the approaches followed by two major state actors – China and Russia - in the process of internet standardisation, and identify patterns of engagement favouring or limiting its 'fragmentation'.

3.3.2. National approaches towards internet standardisation: The case of China

The rise of China as an aspiring technological superpower is the result of a long-term national strategy, building on extensive cooperation with national companies, reforms of its national standardisation apparatus as well as far-reaching influence efforts aimed towards SDOs to favour the advent of Chinese technology at a global level.

After playing a role of catching-up in standardisation arenas (Vialle et al., 2012), Chinese delegations in SDOs are indeed among the largest ones. Chinese presence is said to have recently increased at the ITU level in the field of internet governance (Negro, 2019) and represents 10% of all attendees at the IETF (Hoffmann et al., 2020). Chinese actors are also second (behind the US) in terms of Requests for comments (RFCs) published yearly at the IETF by 2020 (Nanni, 2021). Interestingly, Chinese companies (such as Huawei) have hired senior IETF leaders to rapidly gain social capital and influence within this important SDO (Contreras, 2014). In parallel, the Chinese government is more and more engaging with Chinese non-state actors which are part of these fora, and appears proactive in delegating the advancement of its positions, as evidenced by 'Chinese civil society calls for enhanced state representation and the gradual expansion of Chinese non-state engagement with the IGF' (Galloway & Baogang, 2014). This illustrates China's increasingly strategic approach

towards standardisation processes, as exemplified by its 2018 Standardisation Law and the new China Standards 2035 Plan which call for more Chinese contributions within SDOs. Historically, China has adhered to a rigid top-down approach with regards to standardisation. For instance, it has for years forced Wi-Fi equipment vendors selling on the Chines market to comply with its own WLAN Authentication and Privacy Infrastructure protocol, which was incompatible with international private norms developed by IEEE 802.11, and became the subject of a trade dispute with the United States in the 2000s (Kim et al., 2020).

These policy and regulatory efforts translate the ambition of the Chinese government to develop stronger capacities to formulate its own national standards in the field of digital technologies. The engagement of China within SDOs could thus be viewed as a mean to 'internationalise national standards' (Hoffmann et al., 2020). In addition to SDOs, China also defends its own technological standards and internet infrastructure as part of bilateral cooperation, as well as its Belt and Road Initiative. This far-reaching infrastructural project indeed includes the construction a China-centered transnational network infrastructure (Shen, 2018). This led Seaman (2020) to conclude that China follows a dual approach, combining both cooperation and fragmentation, by developing technical standards through international cooperation processes while facilitating the deployment of its own standards through bilateral cooperation and concrete investment projects'.

In this context, the recent Chinese proposal of a 'New IP' addressing system for the internet (to replace TCP/IP) highlights a move towards a more ambitious approach towards internet standard-setting organisations. This proposal was first presented in 2019 at the ITU's Telecommunication Standardization Advisory Group (TSAG), a policy venue in which China appears to enjoy greater leverage, and thus in an effort to circumvent multistakeholder discussions at the IETF. Promoting a 'decentralised internet infrastructure' (DII), this proposal establishes the technical underpinnings of an alternative and more 'network-centric' internet (Hoffmann et al., 2020). Emphasising the importance of the quality of service (in particular given future internet applications, such as virtual reality) and thus ensuring low latency, this proposal grants more capabilities to network operators and infrastructure providers as compared to the 'end nodes of the internet stack' (Hoffmann et al., 2020). The proposal remains however rather vague from a technical point of view, since only limited details and draft specifications have been shared in the context of ITU study groups. Interestingly, China has framed its proposal as a way to address growing concerns over the consolidation of the internet, by defending on the contrary a 'decentralised' internet infrastructure. Critics of the proposal instead argue that it would 'in fact lead to more centralised (i.e., government) control over networks and users' data' (Hoffmann et al., 2020) and 'is likely to create multiple non-interoperable networks' (Sharp & Kolkman, 2020).

The New IP proposal has been defended at the ITU level by the Chinese technology company Huawei. Huawei is also at the origin of most of Chinese IETF involvement, though more and more Chinese companies are now engaging with its technical discussions (Contreras, 2014). Since many Chinese firms have become technology leaders in various fields (such as artificial intelligence and facial recognition), they appear in a strong position to advance their (often common) interests and standards at the global level. Seaman (2020) reports for instance that China's AI leader SenseTime collaborates with dozens of other Chinese companies to develop national standards regarding facial recognition technologies, while other top infrastructure providers such as ZTE and China Telecom have issued common positions at the ITU level for standards in relation to surveillance technologies.

The exact nature of the autonomy of Chinese companies towards the Chinese government within these arenas is a complex issue (Nanni, 2021). However, under the leadership of Xi Jinping, the links between the Chinese government and leading national technology companies have been clearly strengthened, for instance via the adoption of the 2017 National Intelligence Law. These connections have sparked concerns from many governments, including in the EU, that deploying the technology provided by these firms may affect their national security. These developments should be read as a continuation of Chinese domestic control over its citizens and companies, as

evidenced by the Golden Shield Project (also known as the Chinese Great Firewall). These recent controversies also signal the rising importance of geopolitical games in the development of internet standards. Sanctions issued in 2019 by the US Department of Commerce against several Chinese firms (including Huawei) had for instance led them to be temporarily excluded from a number of SDOs, such as the IEEE (Seaman, 2020).

More broadly, China has advocated for the past two decades in favour of profound changes in the internet governance, calling for a more multilateral decision-making and an increase of government representation. Indeed, the Chinese government has portrayed itself as a long-standing critic of current internet governance mechanisms, which Chinese policymakers have at times characterised as a set of unelected bodies aligned with 'Western' interests. The recent scholarship on the Chinese approach towards global internet governance has however added more complexity to this perspective, noting the nuances of the positions defended by Chinese stakeholders in these fora, and also evolutions in Chinese stances towards multistakeholderism (Galloway & Baogang, 2014; Arsene, 2015; Shen, 2016; Negro, 2019; Nanni, 2021). Nanni (2021) for instance documents how China's participation within a mobile internet standard-making forum (the 3rd Generation Partnership Project, 3GPP) has shifted from a form of isolation to full engagement, leading Huawei to become the 'most influential actor in 5G standardisation within the European-born 3GPP without establishing or seeking to establish any alternative standardisation body' (Nanni, 2021).

The following section investigates the approach followed by Russia, another important state actor in relation to internet standardisation.

3.3.3. National approaches towards internet standardisation: The case of Russia

Though 'largely disinterested in strong internet regulation until the 2010s (Kolozaridi & Muravyov, 2021), approaches towards the strengthening of Russia's technological sovereignty have materialised recently into a number of laws and initiatives aiming to shape an 'autonomous Russian Internet'. Since 2014, the Russian government has been particularly active in redesigning its internet infrastructure (coined as 'RuNet'), to not only limit access to specific website addresses or block messaging platforms (such as Telegram) but controlling more directly the internet traffic across its territory. This trend has further accelerated in the wake of the war in Ukraine.

These efforts have translated for instance into the so-called Law FZ-90 for a 'sovereign RuNet' in 2019. This law derives from previous legislative attempts to establish a 'duplicate' internet, that could operate independently from servers based abroad, which had not been adopted due to strong concerns from Russian industry stakeholders (Stadnik, 2021). Claessen (2020) analyses that the Law FZ-90 implies that 'internet traffic within Russia could only go through internet exchange points (IXPs) that are pre-approved by the institution issuing control and supervision of the internet', the federal authority supervising ICTs Roskomnadzor. In addition, it requires internet services providers to install in their networks technical means to ensure the security and integrity of the RuNet (using for instance DPI technologies), while also creating a National Domain Name System (NDNS). Stadnik (2021) notes that the main idea behind the NDNS is 'to ensure that RuNet sites will still be accessible from Russia in case of any problems with global DNS', but the actual implementation and deployment of such a 'state DNS-resolver' remains unclear given the complexity of its internet architecture (Stadnik, 2021) and the diversity of local 'nets' in Russia (Kolozaridi & Muravyov, 2021).

These new measures have been justified by Russian authorities by the increasing threats in terms of cybersecurity and national security stemming from digital technologies and foreign technology companies, thus corroborating the thesis of Claessen (2020) of an increasing securitisation of internet infrastructure. Stadnick (2020) points however the paradox that this 'centralization of RuNet networks management leads to the creation of a point of potential failure, and deterioration in the

quality and speed of internet connections due to extensive filtering does not de facto provide for a stable and resilient RuNet'.

Russia has thus strengthened and centralised its capabilities to control the online information space as well as key internet resources at the domestic level. In addition to the previous deployment of surveillance and filtering technologies to control access to online information (such as deep-packet inspection technology), along with policy measures designed to censor online content and blacklist specific internet resources, Russia has progressively reshaped its 'internet infrastructure to allow for a more direct control of internet traffic' in the mid-2010s (Claessen, 2020). This contributed to the development of a burgeoning domestic market for internet 'black boxes', including systems for intercepting telecommunications (known in Russia as Systems for operative investigative activities, SORM) and traffic filtering solutions (Ermoshina et al., 2021).

This political ambition to protect the Russian internet was also accompanied by a growing focus 'on the 'import substitution of ICT products' for its own national products' (Claessen, 2020), combined with an increased control over Russian internet and technology companies. In 2017, Russia's government for instance imposed to national companies to focus their businesses on the domestic market in order to be independent from foreign influences (Asmolov & Kolozaridi, 2021). Legal requirements to store personal data of Russian citizens on servers located in Russia were also adopted in 2014 (Wijermars, 2021). In addition, the 2016 Yarovaya Law imposed a set of stringent surveillance measures to be implemented by telecom operators, such as the retention of metadata for three years and the storage of all traffic for six months (Ermoshina & Musiani, 2017). In 2021, following its adoption by the Russian Parliament as part of a revision of consumer protection law, the so-called 'law against Apple' came into force and introduced an obligation for smartphones and devices purchased in Russia to come with pre-installed Russian applications.

Yet, behind the discursive concepts regularly channelled by the Russian government, the actual power of Russian authorities towards internet infrastructures and companies, and its capabilities to enforce new restrictive laws, invite for a more nuanced analysis. Indeed, it should be noted that 'close examination of the legislation and its consequences shows not a centralised domination of the Russian network, but a multiplicity of types of control that are partial, fluctuating and sometimes contradictory' (Ermoshina et al., 2021). Several instances, such as the implementation of the so-called Telegram ban in 2018 (Wijermars, 2021), indeed show how political discourse on internet sovereignty in Russia can be 'largely in excess of the actual technical capacities and expertise necessary to execute these ambition' (Ermoshina & Musiani, 2021).

At the internet governance level, Russia advances preferences reasserting states' sovereignty and the principle of non-intervention in the cyberspace. In line with China, Russia tends to support a state-centric model of global internet governance favouring multilateral agreements rather than multistakeholder settings (Nocetti, 2015). This is well illustrated for instance by its unequivocal support in favour of a stronger ITU's mandate in the field of internet governance. Since the years 1990s, Russia has been a vocal participant to these debates, constantly challenging the dominance of US interests in the governance of key internet resources. In the same vein, Russia was the main driving force leading to the creation of the UN's Open Ended Working Group (OEWG) on developments in the field of ICTs in the context of international security, which it used to advance its discourse around state' sovereignty and control in the cyberspace[19].

[19] The working group has adopted in March 2021 its final report. For more, see: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

The war in Ukraine and internet infrastructures

The Russian invasion of Ukraine, which began on 24 February 2022, is also a cyberwar and a war conducted by digital infrastructures. It had a considerable impact on the cyberspace of the countries concerned, due to drastic changes in Internet legislation in Russia and international sanctions which, among other things, led to the departure of many digital companies. On the Ukrainian side, the physical infrastructure is, of course, heavily damaged by the military operations. Massive cyberattacks on government services on both sides are being carried out by citizens, hackers and state agents, and Kremlin-led disinformation campaigns have taken over Russian social media.

Over the past decade, Russia has deployed several measures for Roskomnadzor (RKN), the federal government's communications control body, to expand its jurisdiction. It can now reach into areas as diverse as online content control, the right to block websites, and the registration of blocked websites, which has greatly increased its censorship possibilities.

And this thanks to an important lever of control of the Russian Internet which relates to infrastructure: the Tehnicheskiye Sredstva Protivostoyaniya Ugrozam (TSPU) system, which can be translated as “technical means of countering threats”. Thanks to this system, RKN can significantly slow down or partially block the most popular social networks in Russia. The new system of deep packet inspection (DPI), planned by TSPU and installed on the majority of Russian networks, is currently used to severely slow down or block Facebook, Instagram and Twitter. and block independent media. The goal, of course, is to control the narratives of the ongoing conflict that the Russian state still refuses to call a war.

War also introduces new risks. Ukrainian citizens and Russian anti-war activists share the same threat model, very specific to war, which is the partial or total shutdown of the Internet. In the case of Ukraine, these connectivity disruptions are mainly caused by physical damage to optical cables or cell towers due to current military operations. In the case of Russia, these shutdowns are orchestrated from above, most often by RKN through the TSPU system. As of June 2022, these shutdowns are frequently paralleled with site blockings targeting human rights organizations and independent press and radio stations.

The ever-increasing set of legal and technical constraints that have weighed on the Russian Internet over the past decade have given rise to a set of resistances and adaptations on the part of Russian Internet users, on which the current situation once again sheds light, while enhancing the analogous strategies developed by Ukrainians. For example, despite its dubious-quality encryption, Telegram secure messaging has since February 24, 2022 become the main communication tool for Russians and Ukrainians. It is used to disseminate more or less independent information and first-hand video and photo documentation of the war. It also serves as the main tool for Ukrainians, to coordinate in emergency situations, and for Russian activists, to organize anti-war actions and coordinate support for arrested activists.

This new context also pushes citizens of both countries to seek alternative tools that can be reliable even when the “normal” Internet is down. The prospect of being completely or partially disconnected prompts users to turn to “legacy” protocols and tools such as text messages and regular phone calls, as well as email. Ukrainians call and text loved ones who sit in bomb shelters for many days with no internet, while Ukrainian ISPs work to bring the internet to the bunkers by relying on a “do-it-yourself” dimension and flexibility that has been specific to the Ukrainian Internet for a long time. Opposition media in Russia meanwhile are reverting to “classic” mailing lists to share information about the war, as their websites are officially blocked.

For the majority of people living in a context of war, digital security becomes less of a priority than connectivity: better to have unprotected communication than no communication at all. But groups of users with more advanced technical skills have nevertheless initiated digital "migrations" and are advocating for greater use of decentralized encrypted messaging services such as Briar, Matrix or Delta Chat.

In light of these clear examples of how states are increasingly taking strategic approaches towards the internet and its standards, as well as the nature of the technical and commercial drivers fuelling the fragmentation of the internet, the following section investigates what is currently the EU approach towards the internet in the context of recent legislative proposals, and their main implications for the protection of an open and global internet.

4. The EU and internet fragmentation

The growing number of legislative proposals on the EU agenda and political importance of internet-related issues for EU leaders have implications for the patterns of internet fragmentation identified in the report. Indeed, core concepts of the EU such as the Digital Single Market (DSM) imply internet convergence within the EU, while others such as digital sovereignty may imply fragmentation at a global level. These political aims do not fully overlap, but are not necessarily contradictory. The literature on the process of Europeanisation and the Brussels effects indeed shows that when the EU exports standards at the global level (Newman, 2008), initial divergences in the form of raised legal standards can pave the way for subsequent convergence through spill-over effects across the world, as well illustrated by the case of the General Data Protection Regulation (GDPR).

Internet fragmentation and the EU's GDPR

During the discussions leading up to the adoption of the EU's General Data Protection Regulation (GDPR), European data protection law has been accused of contributing to Internet fragmentation. When it came into force, the Internet Society argued that the trends reflected by this regulation would 'inevitably lead to fragmentation' (Komaitis, 2018) while Fortune published an article titled 'The GDPR and Our Balkanized Internet' (Roberts, 2018).

When the first EU Data Protection Directive was adopted in 1995, its aim – as for the GDPR – was to protect the fundamental rights to privacy and data protection, but also to ensure the free movement of personal data within the EU single market (Dumont, 2011). Providing adequate protection to fundamental rights related to the processing of personal data was needed from the perspective of several national data protection laws in order to establish the free flow of personal data within the European Economic Community (EEC) and was seen as an important pre-requisite for the creation of the 'Schengen Information System' (Newman, 2008). With the GDPR, adopted in 2016, also came the right to portability, which was designed as an incentive to the development of interoperable formats.

Despite divergences in the implementation of the GDPR, European data protection law has become a unifying factor at the European level. But did it create fragmentation at a global level? Even before the GDPR was adopted, controversy arose when the CJEU ruled that data subjects have a right to be forgotten under the 1995 Data Protection Directive (Case C-131/12 Google v AEPD, May 13, 2014). This meant that individuals could ask a search engine to de-reference pages containing personal data related to them, in accordance with the right to object to processing of personal data based on the legitimate interests of the data controller. Jonathan Zittrain argued that because of this ruling, 'search engines may find themselves in a cat-and-mouse game of censorship and evasion, leading only to a fragmentation, not an improvement, of the web' (Zittrain, 2014). In September 2019, the CJEU added that a search engine 'is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request' (Case C-507/17 Google v CNIL, September 24, 2019). This latter ruling can therefore be understood as directly contributing to the fragmentation of the Internet-as-a-public-space.

Since the GDPR came into force, several websites, especially in the United States, have rendered their pages unavailable to visitors connecting with a European IP address. This choice was made in order to avoid falling into the extra-territorial scope of European data protection law. However, it must be reminded here that neither de-referencing nor blocking access to European IP addresses creates fragmentation at the level of the network. The use of Virtual Private Networks (VPNs) easily allows one to circumvent measures that affect the content of information available to European Internet users. It is also important to take into account the ability of the EU to develop international norms when analysing the effect of European data protection law with regards to fragmentation. As it has been shown by several studies (Newman, 2008; Rossi, 2021), EU data protection law, including the GDPR but also Convention 108 of the Council of Europe, appears to have set the global norm for international data protection.

The following section presents a brief description of the EU's past history in engaging with the standardisation of the internet, and then explores the EU's current approach in relation to its fragmentation, through the analysis of four recent legislative proposals presented by the European Commission since 2020.

4.1. The EU and internet standardisation

Since the 1990s, the EU has been active in the field of standards regulation, notably through ETSI, as well as European Committee for Standardisation (CEN) and European Committee for Electrotechnical Standardisation (CENELEC). EU decisions and legislations (such as the 2012 Regulation on European standardisation[20]) but also case law from the Court of Justice of the EU (CJEU)[21] illustrate the evolving approach of the EU towards SDOs, and the gradual formal recognition of their standards by EU institutions. For instance, in 2010, the European Commission issued guidelines on horizontal cooperation agreements to set criteria for SDOs (such as open membership) and provide a safe harbour for SDO agreements.

The European standardisation system (ESS) is often seen as one of the cornerstones for the completion of the EU's single market as well as a strategic instrument to ensure European and global standards are in line with EU interests and values. Yet, the European Commission has recently recognised that the ESS is not sufficiently equipped to anticipate future standardisation needs, particularly in relation to EU's goals related to the 'Digital Decade'. The new Communication of the European Commission for a new standardisation strategy intends to address this gap, and is framed by the European Commission as a channel to address a 'situation where the respect for core European values and freedoms, in particular in the setting of internet standards and new technologies like artificial intelligence, blockchain, data or online platforms, is being challenged'[22].

Despite these challenges, it should be recognised that the EU has been an instrumental actor in relation to internet standards in a wide range of issues such as the deployment of IPv6 (as seen earlier) and the formulation of the standard 'Do Not Track'.

[20] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

[21] See for instance the 2015 Huawei v ZTE ruling on SDO policies.

[22] For more, see: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy_en.

The EU and the DNT standard

The 'Do Not Track' (DNT) open web standard provides the ability to Internet users to communicate advertisers their will to not be tracked when accessing a particular website. Though it has failed in 'being widely accepted and implemented' (Rossi, 2021), this standard has remained a constant object of contention over the past decade. It originates from the years 2000s, following the public mobilization of digital rights movements such as the Electronic Frontiers Foundation (EFF) and emerging scandals connected to online tracking. The success of this campaign towards U.S. and EU policymakers led to the ushering of a phase of design and creation of a DNT standard in the context of the W3C. As reported by Harcourt et al. (2020), a number of EU public figures, such as European commissioner Viviane Reding, had shown their support to this initiative.

Divergence of positions between the stakeholders involved in the W3C (such as advertisers' coalitions or Google) have complicated the design of this standards, and greatly weakened its initial ambition to address the root causes of online tracking. The standardisation process was eventually completed 'without widespread adoption by online services and major online advertisers have indicated that they will not modify tracking behaviour in response to a user's expressed preference' (Doty, 2020). As such, an industry-approved standard failed to materialize in this context, partly due to the strong incentives for ad tech companies and publishers to not alter their tracking business and affect their ever-growing revenues. Faced with this failure, several privacy organisations launched online tools that would allow users to implement DNT solutions, but without the support of large stakeholders.

In order to address this challenge of acceptance and compliance, California has adopted legislation that forces website operators to provide transparency on how they respond to the DNT signal. The EU Commission's initial proposal for an e-Privacy Regulation, published in 2017, also contained provisions that would have given legal recognition to the DNT signal. DNT was actively supported by the European Parliament, including by Jan Philipp Albrecht, the rapporteur for the General Data Protection Regulation (GDPR) between 2012 and 2016 (Rossi 2021). Yet, there is an ongoing challenge of compatibility and alignment of the DNT standard with existing EU legislations (O'Neill, 2018; Kosta and Kamara 2016), such as the General Data Protection Regulation and the new ePrivacy regulation. Ultimately, the W3C officially dropped support for DNT at the end of 2018, as did the Council of the European Union in its position on the e-Privacy Regulation. This may change, however, should the European Parliament choose to debate the Council's position, and reaffirm support for either DNT or other alternative mechanisms that have been proposed, like the Global Privacy Control or Advanced Data Protection Control.

Interestingly, the original intention of the EU executive to adopt internet SDOs standards as official European ones (in view to include them into EU public procurements for instance) had been met with very negative responses. As a result, one of the ambitions of the 2012 Regulation on European standardisation was to 'accredit existing SDOs' (Harcourt et al., 2020) without necessarily giving a formal recognition to their standards as European standards. This is the reason why this regulation defines standards as "voluntary technical specifications for products, production process, or services'. This emphasis on *voluntary* specifications is important in the context of international trade law. Indeed, one of the provisions of the Agreement on Technical Barriers to Trade (TBT) of the World Trade Organisation (WTO) states that:

> *'Where technical regulations are required and relevant international standards exist or their completion is imminent, Members shall use them, or the relevant parts of them, as a basis for their technical regulations except when such international standards or relevant parts would be an ineffective or inappropriate means for the fulfilment of the legitimate objectives pursued, for instance because of fundamental climatic or geographical factors or fundamental technological problems' (art. 2.4. TBT)*

Therefore, except in rare cases due to a lack of existing interoperable standards, i.e. in the case of standards for payments in the frame of the Single Euro Payments Area[23], the EU has historically abstained from prescribing specific technical standards. Instead, it has strived to find a compromise between the top-down approach adopted by China and market self-regulation, by setting incentives towards the voluntary adoption of ICT standards, and by, at times, taking part in the standardisation efforts (Peng, 2018).

4.2. Current EU approach and legislative developments

As part of its 2015 Digital Single Market Strategy[24], followed recently by the 2030 Digital Compass[25], the EU has increasingly committed to address the many challenges associated with the digital transformation, notably through standardisation and policy initiatives. A myriad of policy proposals is currently under discussion in view to complete the digital single market, define the rules and norms applicable to the digital world globally and strengthen the EU's potential to compete in this sector.

Though the scope of this report is focused on recent legislative developments at the EU level, a series of new EU initiatives in relation to the promotion of an open and global internet also need to be acknowledged. As part of its new Cybersecurity strategy, the EU has for instance announced in 2021 its DNS4EU initiative to support the development of a public European DNS resolver service. DNS4EU is primarily funded via the new EU's Connecting Europe Facility (CEF2). As already identified in previous chapters, the market of DNS resolver services is characterised by patterns of consolidation, with the consequence that EU entities increasingly rely on a few DNS resolvers operated by non-EU services. This has important implications in terms of data security and compliance with EU data protection rules. The DNS4EU initiative intends to address this challenge and contribute to 'secure Internet connectivity by supporting the development of a public European DNS resolver service'[26]. Since July 2021, the new EU-US Trade and Technology Council (TTC) aims at enhancing transatlantic cooperation in the development of compatible and international technology standards. Cooperation is envisioned through the alignment of EU-US positions within international standard-setting bodies. These standards refer in particular to artificial intelligence as well as the internet of things. More recently, in December 2021, the European Commission also announced the launch of a plan for developing its 'Global Gateway'. This plan consists in a range of investment commitments in global infrastructure, including in 'digital infrastructure' such as submarine and terrestrial fibre-optic cables, space-based secure communication systems and cloud infrastructures. In this context, EU investments will be linked with 'standards and protocols that support network security and resilience, interoperability, and an open, plural and secure internet'[27].

In addition to these non-legislative developments, the following section identifies the most relevant EU policy and legislative developments in relation to the fragmentation of the internet. The scope of the analysis of the EU policy space includes relevant policies, including e-commerce, data protection, cybersecurity and other digital policies. The review covers only a subset of recent and

---

[23] See Regulation 260/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009.

[24] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A digital single market strategy for Europe (COM(2015) 192 final).

[25] 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 (COM(2021) 118 final).

[26] Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final.

[27] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank: The Global Gateway. JOIN/2021/30 final.

ongoing EU legislative processes, and focus specifically on the recently proposed EU's DSA, DMA, AI Regulation and NIS 2 directive. This section identifies the main issues related to the fragmentation of the internet, and assesses their possible positive or negative implications.

Table 1: Legislative dossiers under study

Legislative files	Procedure
Artificial Intelligence Act	2021/0106(COD)
Digital Markets Act	2020/0374(COD)
Digital Services Act	2020/0361(COD)
NIS 2 Directive	2020/0359(COD)

These legislative files correspond to the policy dossiers with the most direct implications for the openness and unity of the internet. However, it should be highlighted that a series of other ongoing and upcoming EU negotiations may also be relevant for processes of internet fragmentation. For instance, current discussions on the EU 'e-evidence' package[28] aim at reshaping cross-border access to electronic evidence by judicial authorities in view to grant more power to EU member states when accessing the data of (non-EU) service providers operating in the EU. This new regime would thus have an extraterritorial dimension, and potentially reinforce the already identified pattern of internet alignment. Similarly, negotiations on the draft 'e-Privacy' Regulation[29], related to the protection of personal data in electronic communications, could have great implications on the practices and technologies used by service providers outside of the EU (regarding *cookie walls* for instance) to protect the confidentiality of communications. Also, the recently proposed Regulation for a European Digital Identity (eIDAS Regulation)[30] signals the ambition of the European Commission to foster European standards in relation to electronic identification and website certification, that may very well spill-over at a global level. Recent discussions on the proposed Data Governance Act (DGA)[31], one of the core components of the new European strategy for Data[32], also point to the likely emergence of integrated EU data spaces, leading thus to forms of fragmentation in relation to data governance externally. In addition, the recently proposed Directive on the Resilience of Critical Entities (Directive CER)[33], which complements the revision process of the Directive NIS, could also have great implications for internet infrastructure providers, including internet exchange points and DNS providers. Finally, the European Commission has launched

[28] Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. COM/2018/225 final - 2018/0108 (COD).

[29] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final - 2017/03 (COD).

[30] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final).

[31] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). COM/2020/767 final.

[32] 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data' (COM(2020) 66 final).

[33] Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. COM/2020/829 final.

negotiations on a proposed EU Data Act, which could redefine existing frameworks and introduce new standardised norms for data sharing.

Bearing in mind the recent intensification of the EU agenda on these issues, this review will explore in greater details four key legislative negotiations, starting with the Digital Markets Act (DMA) introduced by the European Commission in December 2020.

4.2.1. Digital Markets Act (2020)

The proposed Digital Markets Act aims at preventing online 'gatekeepers from imposing unfair conditions on businesses and consumers and at ensuring the openness of important digital services'. Among the measures proposed by the European Commission in this proposal, a number of provisions push towards more transparency and contestability requirements to be implemented by large internet platforms. At the core of the proposal is the ambition to address the competition issues posed by mostly non-EU-based monopolies in the digital economy.

Issues relevant to internet fragmentation

Interoperability is conceptualised in this legislative proposal as one of the main leverages to level the playing field between all actors. Given what are the main drivers of the consolidation of the internet infrastructure, namely the concentration of digital markets by a small number of actors and the *de facto* privatisation of key internet resources by a subset of the same internet companies, new rules aimed at limiting the market power of digital monopolies may help in building a more open internet.

There is an ongoing debate about whether minimum requirements for interoperability should be introduced for digital gatekeepers, and on whether technical standards should be defined and implemented at the EU level. This is well illustrated by the recent proposal of the DMA's rapporteur MEP Andreas Schwab (EPP, Germany) stating that 'the implementation of gatekeepers' obligations related to access, installation, portability or interoperability could be facilitated using technical standards. In this respect the Commission should identify appropriate, widely-used ICT technical standards from standards organisations as foreseen under Article 13 of Regulation 1025/12 or where appropriate ask/request European standardisation bodies to develop them'.

The DMA proposal provides a number of other obligations for gatekeepers, including allowing users to install or des-install third party software applications or software application stores. Such measure would help to limit the fact that users may have significantly different online experiences due to the constraints imposed by their app stores and operating systems. In particular, it aims at preventing that gatekeepers' ability to technically restrict how users switch between and subscribe to applications and services using their operating systems. So far, the DMA proposal stops short, however, of providing full support for device-neutrality as it gives manufacturers to sell hardware bundled with the operating system, without giving the user any choice or any transparency on the compatibility with competing operating systems.

The DMA could be an efficient instrument to limit the ossification of gatekeepers' services and support innovation and competition in the digital economy. The introduction of interoperability requirements needs however to take into account data protection rules and other negative impacts, including in relation to competition aspects. Interoperability can indeed paradoxically become a driver for more market concentration, as shown by previous studies on identification services (Riley, 2020).

Future implications

The proposed DMA could help to curb the way by which large internet platforms benefit from their control over the different layers of the internet infrastructure. Yet, the Commission draft legislation

has been criticised for prohibiting the introduction of more stringent obligations for gatekeepers, that would go beyond the adopted DMA.

As emphasised earlier, favouring interoperability requirements could have ambivalent consequences and requires a balanced approach. Yet, the current proposal does not call for a sufficient level of interoperability. For instance, it introduces new obligations for gatekeepers, but only for their ancillary services (such as payment processing). As pointed out by the Bureau Européen des Unions de Consommateurs (BEUC), 'the majority of the obligations and prohibitions imposed on gatekeepers in Article 5 and 6 are aimed at enabling business users to offer services in vertical or ancillary markets, rather than fostering the emergence of new platforms to enable consumers to choose alternative core platform service providers and therefore genuinely creating competition in such services and not only in ancillary ones'. Similarly, the current proposal bans tying an intermediation service to the use of an identification service provided by the intermediary. However, this measure is not extended to other services that could be provided by another service of a gatekeeper.

As suggested by BEUC, large internet platforms have taken advantage of the 'common open standards that have allowed the Internet to flourish', and this open interoperable approach needs now to be replicated by them, including social networks, instant messaging services and cloud services (BEUC, 2021). In relation to communication services (such as instant messaging apps), another possible avenue is to build up on the new European Electronic Communication Code (EECC) provisions and introduce an interoperability requirement for gatekeepers' services that are social media or number independent interpersonal communication services, in the same way as voice and SMS communications, services that come already with interconnection and interoperability requirements from EU telecom rules.

Finally, the proposal has also led to debates around the plans of Google and Apple to end support to third-party cookies in their respective web browsers, notably through Google's FLoC and Topics API projects. This shift is likely to benefit to several companies (Google and Apple) providing web browsers, at the expense of other competitors. This could have not only an impact on market consolidation patterns, but also in the way internet users can express their consent online in relation to data processing, individual tracking and customisation.

4.2.2. Digital Services Act (2020)

Launched simultaneously with the Digital Markets Act proposal by the European Commission in December 2020, the draft Digital Services Act (DSA) intends to lay down harmonised rules on the provision of digital services in the EU's internal market. This legislation aims at reforming the existing legal framework applicable to such services laid down in the e-Commerce Directive 2000/31/EC. More specifically, the proposal introduces a number of new rules, for instance on specific due diligence obligations, tailored to certain specific categories of providers of intermediary services, as well as safeguards for users, including the possibility to challenge platforms' content moderation decisions. The DSA intends to harmonise rules at the EU level, after a number of member states successively adopted diverging national legislations to tackle illegal or 'harmful' online content, such as Germany's Network Enforcement Act (NetzDG) or the Law on Countering Online Hatred in France.

Issues relevant to internet fragmentation

In terms of its territorial scope, the proposed Digital Services Act has extra-territorial effects and may thus foster forms of internet fragmentation. The legislative proposal applies to intermediary services provided to recipients that have their place of establishment or residence in the Union, irrespective of where the providers of those services are established.

There has been a debate on whether core internet infrastructure operators should be part of the scope of the liability regime for intermediary service providers in the DSA, including operators providing DNS services and those involving routing/forwarding, such as internet exchange points. By 'targeting the service providers who are best able to satisfy notice and takedown obligations while minimising the potential for collateral damage to other services or operations' (RIPE NCC, 2021), it appears that the DSA proposal does not threaten the public core of internet, as initially feared by the technical community (RIPE NCC, 2020). Indeed, recital 27 of the proposed act states that:

> *'Since 2000, new technologies have emerged that improve the availability, efficiency, speed, reliability, capacity and security of systems for the transmission and storage of data online, leading to an increasingly complex online ecosystem. In this regard, it should be recalled that providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions, can also benefit from the exemptions from liability set out in this Regulation, to the extent that their services qualify as 'mere conduits', 'caching' or hosting services. Such services include, as the case may be, wireless local area networks, domain name system (DNS) services, top–level domain name registries, certificate authorities that issue digital certificates, or content delivery networks, that enable or improve the functions of other providers of intermediary services. Likewise, services used for communications purposes, and the technical means of their delivery, have also evolved considerably, giving rise to online services such as Voice over IP, messaging services and web-based e-mail services, where the communication is delivered via an internet access service. Those services, too, can benefit from the exemptions from liability, to the extent that they qualify as 'mere conduit', 'caching' or 'hosting service''.*

Nonetheless this provision remains unclear whether DNS services are indeed included in the scope or not, since they do not necessarily qualify technically as 'mere conduits', 'caching' or hosting services'[34]. It can be argued that DNS services have practically no control over the content that is transmitted via their services. Given the potential negative impact of this measure for internet openness, the exemption of core internet infrastructure services from DSA rules could be made more explicit, notably by excluding as internet infrastructure services or cloud service providers in the definition of online platforms, while ensuring that DNS registration are guaranteed to benefit from liability exemptions. Indeed, imposing intermediary services obligations to DNS services appears to contradict the EU's vision of a single and open internet and its commitment to the multi-stakeholder approach in internet governance.

The DSA addresses directly the issue of standard-development in one of its provisions, in view to address the closed nature of internet platforms and the resulting algorithmic amplification and corresponding harms for users. Indeed, article 34 of the proposed DSA invites the Commission to 'support and promote the development and implementation of voluntary industry standards set by relevant European and international standardisation bodies'. These voluntary industry standards would address in particular (a) the electronic submission of notices under Article 14; (b) electronic submission of notices by trusted flaggers under Article 19, including through application programming interfaces; (c) specific interfaces, including application programming interfaces, to facilitate compliance with the obligations set out in Articles 30 and 31; (d) auditing of very large online platforms pursuant to Article 28; (e) interoperability of the advertisement repositories referred to in Article 30(2); and (f) the transmission of data between advertising intermediaries in support of transparency obligations pursuant to points (b) and (c) of Article 24. By promoting voluntary industry standards, this provision has been criticised by various actors, including BEUC[35],

[34] Interestingly, in relation to DNS services, a suggestion has been raised to introduce a fourth category of intermediaries for 'network directory services'.

[35] For more, see: https://www.beuc.eu/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf.

for failing to propose standards which would be subject to transparent, multistakeholder and inclusive processes. The EDPS also called co-legislators to promote the role of European standardisation organisations to draw up interoperability standards, in line with the applicable legislation on European standardisation[36].

In the proposed legislative draft, standards are expected to facilitate the interoperability of advertisement repositories, and thus benefit to relatively small providers of intermediary services. Nonetheless, the DSA proposal does not introduce 'minimum interoperability requirements for very large online platforms, with explicit obligations on very large online platforms to support interoperability, as well as obligations not to take measures that impede such interoperability', as suggested by the recent EDPS opinion on the DSA[37].

Finally, the DSA negotiations have been used by a number of actors to revisit one of the key principles of the 2001 e-Commerce Directive, namely the country of origin principle. Under this principle, service providers are subject to the jurisdiction of their country of establishment in the EU, and not of their country of destination. A coalition of member states, led by France, supports this change which would grant their national authorities more leverage to enforce rules on digital services[38]. The outcome of this negotiation is likely to have a direct impact on the level of enforcement of the rules proposed in the DSA, for instance via take-down orders within and outside the EU.

Future implications

Several aspects of the text related to its territorial scope and enforcement mechanism could have a direct impact on patterns of internet fragmentation. In relation to the removal of content based upon decisions of national judicial or administrative authorities, the proposed DSA limits the territorial scope of such order 'on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, does not exceed what is strictly necessary to achieve its objective'. This provision would have mixed effects in relation to internet fragmentation, as it would further increase divergence in the content available to internet users within and outside the EU, while preventing that states could dictate the content that users based in other parts of the world could have access to. Also in relation to the territorial scope of the legislative act, article 11 of the proposal states that 'providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate, in writing, a legal or natural person as their legal representative in one of the Member States where the provider offers its services'. As such, this measure could be conducive of more fragmentation, as not all websites' operators may be in the capacity or willing to establish a representative officer in the EU and may thus have a splintering effect on users' universal access to information.

In relation to individual splintering, one of the provisions of the DSA (Article 24) introduces new obligations for digital services in relation to online advertising. More specifically, the proposed legislative act states that platforms should be required to provide 'meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed'. As such, the DSA does not regulate ad targeting and profiling, but aims at increasing transparency around such practices. The DSA also introduces a right for users to learn about the main parameters used in recommender systems and a right to opt for a system that is not based on profiling (Article 29).

---

[36] For more, see: https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

[37] For more, see: https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

[38] For more, see: https://www.euractiv.com/section/digital/news/ireland-draws-a-red-line-on-country-of-origin-principle-in-dsa/.

4.2.3. NIS 2 Directive (2020)

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy, which included the new legislative proposal for a Directive on measures for high common level of cybersecurity across the Union (the revised NIS Directive or 'NIS 2'). Due to new cybersecurity threats as well as issues of implementation and enforcement, this legislative proposal aims at revising the current Directive on security of network and information systems which entered into force in August 2016. The proposed NIS 2 directive broadens its scope, aims to strengthen the security requirements imposed and has stricter enforcement requirements including harmonised sanctions regimes across Member States.

Issues relevant to internet fragmentation

The proposed expansion of the scope covered by the NIS2, which obliges more entities and sectors to take measures, also introduces new rules for key internet resources and entities. More specifically, the scope of digital infrastructure considered as 'essential entities' has been broadened to include cloud computing service providers, data centre service providers, content delivery network providers, trust service providers and providers of public electronic communications networks. In particular, the proposal for a revised NIS Directive applies to all DNS service providers, considered as essential services, including recursive resolvers and operators of authoritative servers for the root zone, top-level domains (TLDs), and all other domain names below the TLDs[39].

This proposal has sparked a lot of debates about the implications of the expansion of the directive' scope for the internet, especially given the proposed inclusion of root name servers. Root name servers indeed fulfil an important function in 'maintaining a global non-fragmented DNS for the Internet' (ISC, 2021). They identify the hostnames and IP addresses of the authoritative DNS servers operated by each of the domain name registries that administer all Top Level Domains (TLDs).

Published in May 2021, the draft report[40] of the European Parliament's Committee on Industry, Research and Energy (ITRE) argued in favour of the exclusion of root name servers from the scope of the NIS 2 Directive, in opposition to the Commission proposal. This draft report even states that 'since the Internet grew in the 1970s, 1980s and further, these services are operated by good expert-volunteers. As this service is not monetised, and as it can be argued that governments should not regulate it, the Rapporteur believes that root servers should be excluded from the scope', adding that 'regulating them is contrary to the EU's vision of a 'single, open, neutral, free, secure and un-fragmented network' and could encourage and empower states advocating for a top-down, state-controlled Internet governance approach, instead of the multi-stakeholder approach'.

More specifically regarding DNS providers, the ITRE draft report also proposed to specify further the scope to include 'recursive domain name resolution services for internet end-users and authoritative domain name resolution services as a service procurable by third-party entities'. The argument of ITRE's rapporteur is that distinguishing 'between recursive and authoritative domain services is necessary in order to exclude from the scope organisations that run their own DNS, including individual computer enthusiast'. This proposal is in line with experts' assessment that 'by not distinguishing between 'recursive' and 'authoritative' domain name resolution services in the

[39] For more, see: https://www.icann.org/en/blogs/details/eu-initiatives-relevant-to-the-dns-and-dns-service-providers-feedback-period-still-open-2-3-2021-en.

[40] European Parliament's Committee on Industry, Research and Energy (ITRE), Draft report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.(COM(2020)0823 - C9-0422/2020 - 2020/0359(COD)), 2021.

definition of 'DNS service provider' in Article 4 (14), the proposed Directive does 'bring considerable changes in terms of coverage of entities"[41].

The ITRE draft report also called for the use of 'interoperable secure routing standards' and insisted 'relevant stakeholders including Union businesses, internet service providers and browser vendors should be encouraged to adopt a DNS resolution diversification strategy'.

The territorial scope of the legislative proposal is subject to debate. In the proposal, the revised directive would apply to non-EU entities. In its article 24, the proposed directive states that if:

> *an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive.*

Future implications

One of the main implications of the proposed NIS 2 directive for the internet revolves around the controversial issue of its scope. Among other leading internet stakeholders, ICANN has voiced its concerns over the proposal' scope, in particular due to its implications for the root name service. Available to all users of the DNS regardless of location, this service has operated since the creation of the DNS in the mid-1980s. It is provided by 12 independent organisations around the world on a voluntary basis at no cost to the users of that service[42]. Among them, two are based in the EU (RIPE-NCC in the Netherlands and Netnod in Sweden). The proposed directive would thus imply that in 10 of 12 cases, extra-territorial, regulatory oversight would be applied by the EU. ICANN argued that it is thus possible such voluntary service would no longer be feasible, resulting in a potential fundamental restructuring of how root name service is provided with unknown long-term consequences (ICANN, 2021). In addition, it has been argued that 'should these non-profits decide to abandon root server operation for Europeans, because they can't comply with the compliance procedures or potential fines, their role might well be taken over by parties with large existing compliance desks'[43], thus, fostering further dynamics of consolidation. Also, RIPE-NCC has commented that this provision, favouring extra-territorial regulatory oversight, is likely to be 'reciprocated by other foreign governments, which would significantly complicate the operation of a fundamental component of the internet's global infrastructure – infrastructure that has been extremely resilient, reliable and secure throughout the history of its operation under current conditions'[44]. As such, subjecting the DNS's functioning to government oversight is in contradiction with the 2016 internet Assigned Numbers Authority (IANA) stewardship transition. This refers to the process during which new agreements were established with the Internet community to undertake IANA's functions, following the expiration of the mandate of US authorities. The Internet Systems Consortium (ISC), one of the 12 global operators of authoritative internet DNS root name servers, also argued that that 'any move by a single sovereign state to regulate the RSOs [Root Server Operators] as a group could produce similar regulation by other sovereign states in response. If all RSO operations become regulated simultaneously by multiple sovereign states, the resulting compliance and reporting burdens and the increasing risk of conflicting regulatory requirements

41 For more, see: https://surfdrive.surf.nl/files/index.php/s/aqDquHZMO2SgHWY.

42 The 13 root servers that exist across the globe have 1,396 instances in total, 212 located in the EU.

43 For more, see: https://berthub.eu/articles/posts/dont-ruin-the-root/.

44 For more, see: https://www.ripe.net/participate/internet-governance/multi-stakeholder-engagement/ripe-ncc-response-to-nis-2-directive_march-2021.pdf.

could easily fracture or destroy the root server system as we know it. With its destruction, we fear the destruction of the global unitary DNS addressing system and the fragmentation of the internet that would inevitably follow'[45].

4.2.4. Artificial Intelligence Act (2021)

Launched in April 2021, the proposed regulation on Artificial Intelligence (AI Act) aims at laying down a uniform legal framework for the development, marketing and use of artificial intelligence. One of its objectives is to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values. This legislative proposal aims at strengthening the EU's role in shaping global norms and standards, notably with regards to a trustworthy AI that is consistent with Union values and interests.

Issues relevant to internet fragmentation

While AI is not necessarily part of the infrastructure of the internet as a network, its many applications in the field of IT security or content policy and regulation directly relate to the internet as such. Therefore, although it does not strictly have an influence on internet standards and protocols, it is likely to impact the content and information internet users have access to, as well as on the technologies on which the internet infrastructure relies. In relation to individual splintering, Title II of the proposed act establishes a list of prohibited AI applications. Following a risk-based approach, it differentiates between uses of AI that create an unacceptable risk, a high risk, and a low or minimal risk. Prohibited practices cover AI systems whose use is considered unacceptable, including those having the potential 'to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm'. The proposed act states in its recital 15 that 'aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child'.

In relation to the territorial scope of the proposed regulation (article 2), it is broad as it would apply to providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country; users of AI systems located within the Union; providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union.

The legislative proposal calls for the definition and implementation of new standards for AI systems. Though it does not relate directly to internet standardisation as such, the proposal defines 'common mandatory requirements applicable to the design and development of certain AI systems before they are placed on the market that will be further operationalised through harmonised technical standards'. The proposal reads in particular that 'where harmonised standards do not exist or where the Commission considers that the relevant harmonised standards are insufficient or that there is a need to address specific safety or fundamental right concerns, the Commission may, by means of implementing acts, adopt common specifications'.

[45] For more, see: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F2004650_fr.

Future implications

With regard to AI-based targeting and manipulation, the proposal has been criticised for its limits in providing meaningful protection against fundamental rights violations and individual and collective harms. There is indeed merit to the proposal voiced by EDRi to ensure that the prohibition on subliminal manipulative techniques extends to harms which target groups of people as well as individuals. Indeed, the legislative proposal has been criticised for introducing a loophole in relation to manipulative practices[46]. In the proposed text, in order to be prohibited, AI systems need to deploy 'subliminal techniques in order to materially distort a person's behaviour' or exploits 'vulnerabilities of a specific group due to their age, physical or mental disability' to 'cause or be likely to cause psychological and physical harm'.

The direct implication of the territorial scope of the proposed act is that technology providers will need to comply with EU requirements, or choose not to, leading thus to a possible splintering in the type of services and applications for users outside of the EU. In relation to the formulation of standards for AI systems, the Center for Democracy & Technology (CDT) has criticised the proposal' self-assessment and standardisation approach which could risk absolving public authorities from policymaking, and offloading it to privatised standards instead[47]. Additionally, the French Commission nationale consultative des droits de l'homme (CNCDH) has publicly wondered how the standardisation bodies, first and foremost the European Committee for Electrotechnical Standardisation (CENELEC), would actually transpose the requirements related to fundamental rights into standards.

[46] For more, see: https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/.

[47] For more, see: https://cdt.org/insights/eu-tech-policy-brief-july-2021-recap/.

5. Challenges and opportunities

This section summarises the main challenges identified by the report's review of root causes and patterns of internet fragmentation. Then, these challenges are linked to relevant dimensions of recent EU legislative proposals in order to capture the opportunities and challenges they provide in addressing this phenomenon.

Previous chapters indeed highlight a series of core threats to the unity and openness of the internet, namely technical factors fuelling forms of technical splintering, the increasing ossification of the internet, the problematic organisational concentration in internet governance, the impact of the consolidation of the internet architecture, and the process of internet's alignment with territorial borders.

Technical determinants of splintering

As seen earlier, the development of private addressing systems and the contentious politics behind the deployment of IPv6 clearly show the challenges posed by competition and frictions regarding the compatibility of core technical protocols. The current competition between TLS 1.3 and ETS may give rise to forms of fragmentation for internet users, in terms of the level of security they are provided with when using the internet. In addition, the case of Blink clearly exemplifies the negative effect of incompatibilities at the application-layer for internet universality. Such incompatibilities can be used as strategic tools by technological companies to control digital markets and participate to the shaping of a less interoperable and more fragmented internet. Indirectly, these incompatibilities can also lead to the planned obsolescence of protocols, devices or applications, raising the separate questions of environmental impacts and widening of the digital divide between those who can afford up-to-date equipment and others.

The increasing ossification of the internet

In parallel to forms of technical splintering, recent research also points to challenges posed by the increasing ossification of the internet over the two past decades, following its process of commercialisation (Greenstein, 2017). The process of ossification consists in the 'the decreasing flexibility of the network which results in the inability to deploy a new protocol or protocol extensions due to the unchangeable nature of infrastructure components that have come to rely on a particular feature of the current protocols' (ten Oever, 2020). This process can be partly explained by the introduction of so-called 'middleboxes' by network operators to control and optimise the traffic, which have had the negative externality of hindering the deployment of new protocols, that would not be recognised by firewalls for instance. In other words, the 'ubiquity of middleboxes of a variety of forms (from Network Address and Port Translators (NAPTs) to firewalls, accelerators, load-balancers, and a range of portals and more exotic devices) makes it very hard to change the status quo' (Papastergiou, 2016). As convincingly argued by ten Oever (2020), this situation constrains the internet protocol community and end users while granting more control to network operators. This is in this context that the development of the QUIC UDP internet connections (QUIC) needs to be understood, as this protocol specifically intends to circumvent (as much as possible) other parties located between endpoints of a connection. Nevertheless, the genealogy of this protocol, its prominent initiator (Google) and the fact that its success largely builds on Big Tech's consolidation of various points of the internet stacks indicate that concerns regarding the consolidation of the internet architecture should be fully addressed.

Organisational concentration in internet governance

Technological companies can be indeed important drivers or catalysts of internet fragmentation, as their commercial interests may enter in conflict with the goal of ensuring the unity and openness of the internet. In this report, the ongoing deployment of QUIC is presented as an instance of how protocols may contribute to internet consolidation, though with important nuances. Another case underlines the growing concentration of DNS resolution services and shows how this pattern has a direct impact for internet universality, given the capabilities it provides to a few corporate actors in resolving all the internet traffic. Previous sections emphasise that one of the main challenges in this context revolves around the increasing organisational concentration of few actors within standard-making bodies, and in particular the unique role played by internet monopolies in these fora. It illustrates the great power of large technological companies in the making process of core components of the internet stacks. Key SDOs in internet governance, like the IETF and the W3C, and other key actors like the ICANN, are weakened when a single actor concentrates enough market of infrastructural power to circumvent its consensus-seeking processes and are able to impose the use of a certain standard or a certain technology, without providing neither full interoperability nor royalty-free access required by participation in these same organisations. This has been illustrated multiple times over the history of the internet. Supporting the work of multi-stakeholder organisations that provide free and open standards should be a priority if the aim is to maintain an open and universal internet.

Consolidation and internet resilience

As emphasised earlier, the internet was built to be resilient. To achieve this, its designers chose the principle of a distributed end-to-end architecture (Baran, 1964; Musiani & Schafer, 2011). This principle, which has only ever partly been implemented in practice, has come under pressure to the phenomenon of internet consolidation (Arkko et al., 2019) and 'centralisation'[48] (Notthingham, 2022). Some key actors, including social networks operating single sign-on services like Google and Facebook, cloud service operators like Amazon or OVH and Content Delivery Networks (CDNs) like Fastly or Akamai are now key infrastructure operators. The failure of their equipment has consequences on vast chunks of the internet, affecting global connectivity, and the lives of people relying on their services. Just in 2021, many recent examples of outages caused by the ripple effects of the failure of a single key actor include Fastly in 2021, Facebook in that same year, OVH when one of its data centers burnt down, and Let's Encrypt, which is a key actor in handling security certificates that allow websites to operate securely, failed to extend its root certificate on time. This should be identified as a key area of concern, which is related to the matter of fragmentation. The development and support of federated infrastructure and services may be a path to be explored as a policy option to address this issue.

To address these challenges as well as the waste of resources created by current forms of cloud computing, a new technology called 'fog' or 'edge' computing is being developed by industrial and academic researchers. The fog is not intended to replace the cloud with something else, but rather to extend it to make it more efficient and less energy intensive. The idea is to add additional machines, located as close as possible to the users, in order to shorten the network distances. Using nearby 'fog' servers would significantly reduce the consumption of unnecessary resources. Fog computing would likely prove to be particularly useful in the context of the extremely rapid development of the internet of things, i.e. all the communicating objects present in our daily life, in business, in public authorities, etc. Even though each sensor produces little data, all of the connected objects in the world produce total network traffic that is growing much faster than the

[48] Mark Notthingham defines Internet centralisation as 'the ability of a single entity (e.g., a person, company, or government) -- or a small group of them -- to exclusively observe, capture, control, or extract rent from the operation or use of a Internet function' (Notthingham, 2022).

capacity of the internet. Under these conditions, it becomes essential in the medium term to be able to process these data as close as possible to their place of production. The fog provides an infrastructure very well suited to this kind of needs. The 'turn to fog computing' and the objective to fully leverage the proximity between servers and their users' forces to have servers in a large number of locations so as to cover a given territory. Smaller machines, less expensive, but also less powerful, and arranged at a number of specific and reduced distance from each other: a new environment that must be fine-tuned socially, economically and politically in order to learn how to make the most of it. As Europe fosters initiatives such as GAIA-X and overall expresses the wish that cloud computing be 're-soveregnised' and made more independent from U.S.-based giants, the evolutions of cloud computing in the next years will likely entail the need for appropriate policies at the EU and member state levels.

Internet's alignment and territorial fragmentation

The role of states and their strategic interests to exercise power in and through cyberspace is recognised in this report as a core driver for internet fragmentation. As we have seen, the principle of an open internet may at times be at odds with fundamental principles, such as the right to privacy, human dignity or intellectual property rights. Indeed, when the EU – or other liberal democracies – impose rules on global internet actors, it may affect the availability of certain information within the EU on the internet-as-a-public-space. Yet the challenges raised by the intent of certain states to align internet infrastructure and content with their national interest also raise the question of how to respond to those states that limit connectivity to restrain key freedoms such as freedom of expression. Both China's dual approach in relation to internet standards development (combining both cooperation and fragmentation), and Russia's ambition to redesign its internet infrastructure, are clear examples of how states are increasingly taking strategic approaches towards the internet and its standards to 'recreate the power structures of national governments in cyberspace' (Mueller, 2017). In this context, there appears to be a fine line between designing infrastructure that allows states to impose human rights-based values on the infrastructure through the use of territory-bounded legal instruments, and allowing the same infrastructure to function in a way in which users wanting to escape a walled-off internet imposed by a human-right-violating state actor remain able to do so.

The EU as a catalyser for solutions and threats

In relation to these challenges, the EU legislative agenda is both a driver for positive opportunities but could also become a catalyser for the worsening of the very same threats. The EU Digital Single Market Strategy as well as the more recent 2030 Digital Compass underline the EU commitment to address the many challenges associated with the digital transformation, promoting the development of a single, open, neutral, free, secure and un-fragmented network, while adopting a more strategic approach to the making process of internet standards and protocols. The following section summarizes specific challenges and opportunities for the EU in the context of the recent legislative proposals under study.

Recent EU legislative proposals, such as the Digital Markets Act, intend to address the consolidation of the digital economy and internet architecture. By ensuring the openness of large digital services and increasing competition, the DMA proposal can be considered as an opportunity to address different forms of internet splintering. At the individual level, it could address the fact that users may have significantly different online experiences due to the constraints imposed by their app stores and operating systems. At the commercial level, the DMA could be an efficient instrument to limit the ossification of gatekeepers' services and support innovation and competition in the digital economy. The DMA is also an opportunity to introduce technical standards at the EU level for minimum interoperability requirements, however the current legislative proposal falls short in expanding interoperability requirements to 'core services' for instance. Similarly, the Digital Services

Act can be seen as a relevant venue to promote the role of European standardisation organisations to draw up interoperability standards. Yet, so far, the DSA proposal does not introduce minimum interoperability requirements for very large online platforms that would be considered sufficient to introduce these patterns.

Regulators in the EU increasingly consider interoperability as one of the main available solutions to combat the 'natural forces pushing towards greater concentration' (Riley, 2020). Yet, interoperability needs to be approached critically, and cannot be considered as a one-size-fits-all solution. Even for dominant technological companies, interoperability can appear as a conundrum, as these businesses can 'find themselves on both sides of the debate between those who favour and oppose intervention in support of interoperability' (Simcoe & Watson, 2019). Simcoe & Watson (2019) note for instance that Google has faced legal actions both for 'forking' Java to create the Android operating system and setting anti-forking provisions in its Android licensing agreements (Vezzoso, 2018). Using the example of online identity authentication, Riley (2020) shows that despite a well-established interoperable protocol agreed by the IETF in this field (OAuth 2.0), the dominance of Facebook in the login services provided over this protocol has given to the company a considerable lock-in effect (this applies to Google as well). Indeed, 'if you use your Facebook account as the source of your identity with 20 other websites, and then choose to delete your Facebook account, you risk losing access to those 20 additional services – or at the very least, have substantial work to do to avoid losing access' (Riley, 2020). This instance underscores how interoperability and competition policy frameworks need to go hand in hand to be efficient. Yet, the current legislative proposals fall short in relation to the interoperability requirements that need to be introduced to address these challenges.

In addition, the text of the proposed NIS 2 Directive could be seen as a potential driver for increasing internet's alignment, and thus splintering. Indeed, by including root name servers within its scope, the directive could represent a threat to the global unity of the DNS addressing system. This measure could also have negative effects far beyond the EU. Indeed, if such provision was to be reciprocated by other state actors, this could hinder the operation of a critical element of the internet infrastructure at a global level.

Certain aspects of other ongoing EU legislative dossiers also relate to forms of internet's alignment with territorial borders. This is well illustrated by the fact that the scope of the proposed Digital Services Act is said to include DNS services, such as the DNS root or the root name servers. As a result, the DSA appears to contradict the broader EU's vision in favour of a unified internet and its commitment to the multi-stakeholder internet governance approach. This is the reason why core internet infrastructure services would benefit from being excluded from DSA rules. Also debates related to changes to the 'country of origin principle' in the DSA, which if changed would grant authorities from the 'country of destination' more leverage to enforce rules on digital services, could also fuel forms of internet's alignment. In the case of the AI Act, as for other important EU legislative acts (including the GDPR), the territorial scope of the legislations can lead to forms of internet splintering, since they apply to citizens, companies or products also located outside of the Union. The direct implication of the proposed territorial scope of the AI Act is that technology providers will need to comply with EU requirements, or instead choose not to, thus leading to a form of fragmentation in the type of services and applications available to users and companies outside of the EU.

6. Policy options

This chapter explores policy options for the EU to address the issue of internet fragmentation, looking at a variety of policy instruments. After a brief introduction presenting the framework for the development of policy options and general considerations guiding their assessment, four comprehensive strategic options on internet fragmentation are investigated.

6.1. Introduction

As emphasised by previous chapters, there are many ways in which the EU policies have an impact on the tension between the fragmentation and unification of the internet. Some of these policies have been criticised by certain stakeholders as a driver of fragmentation, especially due to their territorially-bounded rules, data localisation and transfers requirements (Kotaikis, 2017; Smolenskiy and Levshin, 2021), or because of the right to be forgotten (Chenou and Radu, 2019).

Current proposals contain measures that are aimed at tackling the increased centralisation of the internet, and should help counter the tendencies that lead to the development of corporate walled gardens and limit the free flow of information and service diversity. At the same time, initiatives that aim at regulating core internet infrastructure such as the Domain Name System (DNS) have been criticised for their capacity to create competing root domain name records (Musiani, 2016).

It should be highlighted once again that legislation is not the only kind of policy instrument through which the EU may affect the unity of the internet. Although it has usually adopted a rather hands-off approach to standardisation, in line with international trade law and its own 'New Legislative Framework', the EU has at times been able to legally impose standards of its choice, for instance in the field of payments, with Regulation 2012/260.

Regulators have also been known to impose sanctions on operators that were not applying the latest standards, for example in the field of cybersecurity, thereby endorsing certain standards over others and imposing their use. Funding for research, civil society initiatives and for development aid projects may also affect standardisation efforts and access to connectivity. Finally, foreign policy can also affect the unity of the internet. Sanctions imposed by the United States and/or the EU on Iran or Syria, for example, may affect the ability of 'Réseaux IP Européens - Network Coordination Centre' (RIPE-NCC), the regional internet registry for Europe and the Middle East, to provide resources that are critical to internet connectivity (Fragkouli, 2021).

6.1.1. Framework for the policy options

In this report, we have looked with different levels of depth at the following proposals: Digital Services Act, Digital Markets Act, the NIS 2 Directive, and the AI Act. Where relevant, we have also discussed the Data Governance Act proposal, the EUID proposal, and a few already adopted directives and regulsations such as the Open Internet Regulation (Regulation 2015/2120), the General Data Protection Regulation (GDPR, Regulation 2016/679), adequacy decisions based on the GDPR, and the 2019 Copyright Directive (Directive 2019/790).

Almost half of the legislative proposals that we studied have now entered phases of trilogue or at to be formally agreed. Therefore, considering that positions in most of these legislative files have already been adopted, and that the room for new ideas, amendments or adjustments is limited, our research has focused on determining different strategic attitudes that the EU could adopt to develop a consistent approach towards the topic of internet fragmentation. These approaches are classified as:

- **Embracing fragmentation**: in this scenario, the EU would foster the free-flow of data and information within the bloc, but would not restrict itself from setting up barriers

between itself and the third countries, including by imposing its own technical standards and communication protocols where necessary, whenever this would meet a public interest, either on the basis of economic, intellectual property, security or fundamental right interests,

- **Maintaining the status quo**: in this scenario, based on the assumption that the internet and the digital market are structured in a way that prevents any real fragmentation from happening at all, the EU would maintain the current balance between adopting rules on data localisation and transfers and impose some rules on gatekeepers to improve competition, but it would not adopt any new rule affecting the tension between fragmentation and unity of the internet and it would not intervene in the field of standardisation.
- **Consistently fighting fragmentation**: in this scenario, where fragmentation is considered to be something to be avoided as such, the EU would have to revise a lot of its current policies in order to ensure that its rules have no fragmenting effect whatsoever, while ensuring it breaks situations of monopolies that allow certain corporations to create their own walled gardens, and creating instruments to help bring connectivity to countries that limit access to the internet.

Given the difficulty of choosing a suitable approach, and taking into account the fact that some factors leading to fragmentation, like the transfer rules in the GDPR, are there in order to ensure the effective application of fundamental rights that are not an option in the EU's legal order, we have developed a **fourth approach based on human rights** law where internet unity is derived from certain fundamental rights such as the freedom to access information, and any limitation to that right should be, in the words of the European Court of Human Rights (ECtHR), 'necessary in a democratic society.'

For each scenario, we outline potential benefits and drawbacks, the word 'potential' being used as a way to convey that the amount of benefit and disadvantage resulting from the choice depends on one's initial set of beliefs, practical/political positioning and interests.

6.1.2. General considerations guiding the assessment of the policy options

This section has been written with the aim of reflecting a broad and balanced variety of views and interests, independently of the said interests. For the sake of transparency, it is nonetheless necessary to point out that its writers all hold views that are favourable in principle to the unity of the internet. We nonetheless also explored reasons to embrace the fragmentation of cyberspace. Following the principles of communicational approaches to public policy, we have been attentive to linking proposals to the normative set of values and interests that each of them is based on.

Although we have sought to provide as wide an overview as possible, this report has as pre-conditions a few basic tenets of legal and technological soundness that should be preserved in all future scenarios. In particular, our analysis of policy options aims at pursuing two goals:

- being compatible with supra-legal obligations under international or constitutional law, especially human rights law and civil liberties,
- ensuring the continued functioning and resilience of the transport layer of the internet.

Proposals have been assessed based on their compatibility with international and constitutional law in general, and fundamental rights in particular. Indeed, fragmentation of the internet, or its opposite, unity, is a subject matter intersecting with many fundamental rights protected by the EU's Charter, such as privacy (art. 7), data protection (art. 8), freedom of expression and information (art. 11), freedom of assembly and association (art. 12), freedom of the arts and sciences (art. 13), the

right to education (art. 14), freedom to conduct a business (art. 16), the right to property (art. 17), environmental protection (art. 38) and the right of access to documents (art. 42).

Therefore, policy options are examined against the following criteria:

- Does the chosen option increase fragmentation or promote unity?
- Does the chosen option follow a public interest?
- If it does, what is the public interest that is being pursued, and does it relate to a fundamental right recognised by the EU Charter of Fundamental Rights?
- Is the chosen option compatible with international law, including trade law?
- Would the internet still be able to function if this proposal were to be implemented?

This method, which is consistent with views expressed by several stakeholders, leads us to a rephrasing of the problem of internet fragmentation from a technical issue relating to the transport layer of the infrastructure and protocols, to a question related to both:

a) the possibility of citizens to access a convergent, open and interoperable global digital public sphere and market, without obstacles of either technical, commercial or political nature,
b) and a matter of constitutional checks-and-balances in the context of the inscription of liberal democratic values in law and in an infrastructure that fundamentally affects power structures in contemporary societies.

6.2. Comparing comprehensive strategic options on internet fragmentation

In this section, we outline several possible strategies to promote a consistent way for the EU to approach internet fragmentation: (1) maintaining the status quo, (2) embracing fragmentation, (3) consistently fighting fragmentation or (4) accepting fragmentation that is necessary in a democratic society.

We review each of these scenarios against rules laid out in international trade law and EU treaties, looking especially at the compatibility of each scenario with requirements laid out by the Charter of fundamental rights, but also the impact each scenario may have on the continued functioning of the internet.

6.2.1. Maintaining the status quo

Description

In this scenario, EU public policy is not developed with any consistent aim with regards to the matter of fragmentation. The governance of the internet would remain essentially a multi-stakeholder process, and the EU would rarely intervene directly in matters related to standards. Some measures would keep having an impact on the subject matter, as existing rules on transfers, data localisation, accessibility, net neutrality or competition, would remain as they are and would each pursue their own goals in the protection of privacy, data protection rights, digital sovereignty, competition, or consumer protection. The extent of these effects has been discussed in previous sections of this report.

Potential Benefits

This scenario might provide benefits of reducing complexity in the decision-making process, and is suitable if the matter of fragmentation is not considered a priority, a likely risk, or a public problem.

Potential Drawbacks and Legal Hurdles

This scenario is not likely. Proposals set forth in the legislative files that we have examined, proposals to reform the European standardisation strategy, international negotiations on the future of internet governance, and increased pressure from public authorities with regards to the regulation of data transfers, mean that conservation of the current status quo is unlikely.

As it has been pointed out by previous chapters of the report, the reality of fragmentation defined as a total loss of connectivity, at least at the technical level, or even the risk of it ever happening, is subject to debate between experts. However, Russian and Chinese initiatives, combined with a deteriorating international climate for the upholding of an open and global multi-stakeholder process, will lead to fragmentation being on the agenda, either as an opportunity or as a risk. Recent initiatives that aim at imposing design elements in digital infrastructure and services available in the internal market such as upload filters (art. 17 of the 2019 Copyright Directive), or 'lawful filtering' complying with EU legal requirements and national legislation of EU Member states (a requirement in the DNS4EU tender[49]), or to force browsers to recognise Qualified Website Authentication Certificates[50], may mean that some EU policy initiatives contribute to patterns of divergence.

The adoption of a clear strategy would ensure that any effect of EU public policy on patterns of convergence and divergence in the internet is the result of a conscious political choice that respects the EU's obligations under primary law and international law, rather than being left to chance.

6.2.2. Embracing fragmentation

Description

Fragmentation can be the consequence of measures meant to pursue either public or private interests. For example, delisting certain domain names from DNS servers to prevent access to illegal content pursues a public interest but creates fragmentation, Apple's decision to withdraw support for Flash in 2010 or to block one of the protocols used to connect to Virtual Private Networks, the Point-to-Point Tunneling Protocol (PPTP), may serve security purposes, and choosing a proprietary instant messaging protocol over one such as the interoperable Extensible Messaging and Presence Protocol (XMPP), may serve the commercial purposes of an actor big enough not to benefit from interoperability.

In a way, fragmentation has always been part of the design of the internet. This scenario examines what happens if fragmentation and its potential benefits are embraced.

This scenario could involve several options:

- The proposed NIS2 Directive would be adopted in a version that applies to all root DNS servers, as was the initial intention of the European Commission. Upload filters may be used in conjunction with human moderation to delete illegal content from sites that can be accessed from within the European Union, and a European DNS root is created with features that allow public authorities to easily delete entries linking a domain name with the IP address of a server that does not comply with its obligations under the law of the EU or of a Member State.
- Under a reformed European standardisation strategy, following the proposal laid out in the new Standardisation Strategy of the Commission, national standardisation bodies will be the only ones allowed to take part in the decision-making process of

[49] See the Call for the DNS4EU project, referenced under 'CEF-DIG-2021-CLOUD-DNS-WORKS', available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works.

[50] This obligation is contained in the new version of article 45 of Regulation 910/2014 (eIDAS Regulation) proposed by the Proposal for a Regulation amending Regulation 910/2014/EU as regards establishing a framework for a European Digital Identity (EID Proposal, COM/2021/281 final).

European standardisation organisations, in order to avoid the influence of actors from outside the EU and the EEA, especially in key areas related to the internet, like cybersecurity or Artificial Intelligence. Legislation would refer to standards developed by the European Telecommunications Standards Institute, the European Committee for Standardization (CEN) or the European Committee for Electrotechnical Standardization (CENELEC) and require their adoption for any good or service marketed on the EEA's territory. If this approach followed that of China's national WLAN Authentication Privacy Infrastructure standard, which was a competitor to the IEEE's own internationally used specifications, this would mean, for example, that the EU or Member States would have the possibility, to impose the use of ETS (formerly called eTLS), specified by ETSI, over that of TLS, for the encryption of telecommunications.

- 'Schengen routing', defined as the fact that communications between two nodes located in the Schengen area are routed through nodes that are all located in that area (Dönni et al, 2015), could be imposed, e.g. by introducing the necessary provisions in the European Electronic Communications Code or in the proposed e-Privacy Regulation.
- Restricting access to the European fragment of the internet could be used as part of diplomatic sanctions against third-countries.
- Interoperability and data portability requirements would be dropped in existing and proposed legislation, including the GDPR, the proposed Data Act, Digital Markets Act and Digital Services Act.
- Net neutrality and universal access requirements imposed by the Open Internet Regulation would be dropped.

These examples provide a few examples of what this strategy could entail, without being exhaustive.

Potential Benefits

This scenario is based on the premises:

1. That fragmentation is in the nature of the internet itself, and/or

2. That fragmentation is beneficial to digital sovereignty as it allows state-actors to better exercise their powers over the digital public sphere, and/or

3. That commercial walled gardens allow companies to create well-integrated, efficient and user friendly equipment and services, ultimately benefiting the user, and increasing the security of products and services.

Aligning the digital public sphere with the boundaries of European sovereignty – shared between the EU and Member States – can help the EU assert political values, including fundamental rights such as privacy or the protection of intellectual property. A strict enforcement of data localisation rules and rules limiting or banning data transfers to third countries can help considerably limit foreign public or private surveillance on European data, including personal data or data containing information on industrial or trade secrets.

By pushing foreign actors and services that fail to comply with European rules from the internal market, new services can emerge, that may then be able to compete on the global internet market.

Moderation and deletion of illegal content will be helped by the ability to control DNS records and by the development of capabilities by infrastructure and service providers to implement both human and automated filtering capabilities. Restraining access to VPN services, like in China, or to encryption, would cement the EU's capability of filtering online content accessible from its territory.

Developing the capacity to limit access, at the transport layer, to or from certain autonomous systems (sub-networks of the internet) to the European internet, might further be necessary to fully implement a strategy meant at cutting off access to illegal content.

Finally, allowing companies to develop their own integrated digital ecosystems has been presented by the ACT App Association as something that provides stability, usability and security within that ecosystem[51].

Potential Drawbacks and Legal Hurdles

A first risk that has been raised by several experts is that if European rules create a European splinternet, cutting off access to the European Union to third-country actors, then the incentive that now exists to comply with European rules even outside of the EU will be severely limited. This may limit the so-called 'Brussels effect' (Bradford, 2012) that has been particularly strong in the field of data protection (Newman, 2008) and is a powerful political incentive. Even if it does not appear to be a likely scenario on a big scale, it may also lead to disruptions of service for European users if providers of key services, equipment of software that are not produced in Europe, like web browsers, decide to leave the European market.

Imposing standards that diverge from internationally recognised standards may conflict with international trade law. The Technical Barriers to Trade Agreement only allows direct state intervention in technical standardisation when it is done in the pursuit of a limited list of public interests ('national security requirements; the prevention of deceptive practices; protection of human health or safety, animal or plant life or health, or the environment', TBT Agreement, §2.2.). It also lays down a procedure that must be followed to ensure that no standard is imposed unless it is proven that no existing technical standard exists to meet the public interests pursued by the state.

Importantly, it should be noted that although certain aspects of fragmentation may help ensure more efficient application of European law, including most fundamental right guarantees, in the online public sphere, one exception is freedom of speech. Indeed, article 11 of the EU's Charter of Fundamental Rights states, i.a., that the right to freedom of expression and information 'shall include freedom […] to receive and impart information and ideas without interference by public authority and regardless of frontiers.' In 2009, the French Constitutional Council, following a global trend in Europe, ruled that 'in the current state of means of communication, and given the generalised development of online communication services and the importance such services have taken for the participation to democratic life and the expression of ideas and opinions,' freedom of expression 'implies freedom to access such services'[52]. This echoes a decision, from the year, by the European Court of Human Rights (ECtHR)[53].

Mandating the use of specific standards over others risks undermining the security of the internet, as this will limit the capacity of operators to apply the latest technology in the field of cybersecurity. This would for instance appear to be particularly the case if ETS (Enterprise Transport Security) was to be imposed over recent versions of TLS, given that the former, unlike the latter, does not support forward secrecy.

Finally, including restrictions to internet access as part of sanction packages might be counterproductive when the aim of such sanctions is to support transition towards the rule-of-law and democracy in the targeted country.

---

51 See their policy paper on the proposed DMA: https://actonline.org/wp-content/uploads/ACT-The-App-Association-DMA-Position-Paper-March-.pdf.

52 French Constitutional Council, Decision nr. 2009-580 DC of 10 June 2009, pt. 12.

53 ECtHR, Ahmet Yıldırım v. Turkey, no. 3111/10, 18 December 2012, and Times Newspapers Ltd. v. United Kingdom, nos. 3002/03 and 23676/03 §27, 10 March 2009.

6.2.3. Consistently fighting fragmentation

Description

Consistent support for patterns of divergence and the unity of the internet, both as a network of interoperable networks and as a global public sphere, would imply decisions such as:

- Imposing strict interoperability requirements, but allowing market actors to choose the best available open and interoperable global standard used by the industry,
- Give Member States possibilities to introduce more stringent measures with regards to interoperability than what is required as a minimum under EU law,
- Increase the pace of negotiations for adequacy decisions based on the GDPR, or amend the GDPR to drop restrictions on personal data transfers altogether,
- Amending Regulation 2018/1807/EU of 14 November 2018 on a framework for the free flow of non-personal data in the European Union to forbid any data localisation requirements being imposed by Member states,
- Keep the graduated approach to the regulation of online platforms and gatekeepers adopted in the proposed DSA and DMA, in order to ensure that smaller actors can emerge and provide an alternative to current technological silos created by the predominance of a few very large online platforms and gatekeepers,
- Restricting the scope of the proposed NIS2 Directive in order to avoid covering root DNS servers,
- Forbidding the practice of geo-blocking,
- Amending the Open Internet Regulation (2015/2120/EU) to include networks like Cogent or Hurricane Electric, that do not provide services to end-users, but to other networks, including to internet service providers, in the scope of network neutrality obligations,
- Create new long-term instruments for the funding of open sources projects which are structural to the functioning of an open, interoperable internet, such as OpenSSL,
- Adopt a European equivalent to the U.S. Global Online Freedom Act of 2013 to impose transparency and due diligence measures on information society service providers operating in countries that restrict access to the internet,
- Use international cooperation initiatives, such as the new EU Global Gateway, to create incentives for companies and public authorities to support net neutrality, improve data protection adequacy mechanisms and prevent patterns of internet consolidation and fragmentation.

Generally speaking, achieving the aims set forth in this scenario would entail refraining from using legislation to mandate specific technical design or the use of specific protocols over others, and to let market actors make their decisions based on the availability of global open standards. Market consolidation may reinforce the capacity of a given actor to impose its own standards or to break interoperability with products and services from other providers, and can be combatted through measures such as those set forth in the proposed DMA and those already provided in competition law.

Measures to systematically combat fragmentation could include the provision of public DNS or VPN services and other tools to citizens from third-countries wishing to circumvent national censorship of their local segment of the internet, and access a global, more united internet.

Potential Benefits

This approach would be the most suited to support the functioning of the internet as a global, interoperable and decentralised network of networks. This would support maintaining a single global DNS root and routing system, and allow unrestricted access to a united global public sphere and market.

The absence of any mandate to use a given technical standard which may differ from the consensus born in a global multi-stakeholder process makes this scenario compatible with international trade obligations, especially the TBT Agreement. At the same time, this approach does not prevent public authorities from holding market actors responsible if, for example, they choose to ignore the state-of-the-art in terms of cybersecurity standard and data protection by design principles.

This approach would be in line with the duty of the EU to guarantee freedom of expression which includes the right to 'receive and impart information and ideas without interference by public authority and regardless of frontiers' (art. 11 of the Charter of Fundamental Rights) and 'through any media' (art. 19 of the Universal Declaration of Human Rights).

Measures to improve interoperability, including through the use of global open standards, may help in slowing or reversing the process internet consolidation (Arkko, 2020), thereby improving resilience and decreasing the amount of single point of failures that are causing regular disruptions in availability of the internet.

Potential Drawbacks and Legal Hurdles

It may not be possible to drop all data transfer requirements. The CJEU has ruled that they may be required for personal data under art. 8 of the Charter. Indeed, if personal data is held in a third-country that does not provide adequate safeguards, 'it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured'.[54]

The same can be said about the right to be forgotten and to be de-listed, which is derived simply from the existence of a right to oppose data processing operations based on the legitimate interests of a data controller, which itself is derived from the principle of lawful processing prescribed by article 8 of the Charter of fundamental rights. Fragmenting effects of this right is limited by the fact that the CJEU has ruled that search engine entries de-listed under this right should only be removed from versions of global websites with country-level top-level-domains from European countries[55]. It should furthermore be noted that publication on a website should not be qualified as a 'transfer' under data protection law[56].

Other data localisation requirements may be necessary on grounds of public security, as envisioned by the Regulation on the free-flow of non-personal data, to protect intellectual property rights, or other interests that may justify proportionate limitations to the unity of the internet.

6.2.4. Towards fragmentation that is 'necessary in a democratic society'

Description

The unity of the internet may be conceptualised as being related to freedom of expression. Borrowing from Isaiah Berlin (1969), there is a strong 'negative freedom' element that restricts the state's ability to restrict freedom of speech, access to information, and, by extension, to restrict access to (certain portions of) the internet. It should be kept in mind that, according to article 11 of the EU's Charter of Fundamental Rights, freedom of expression includes the right 'to hold opinions', 'to impart' them without interference from public authorities, but also to 'receive information […] and ideas […] regardless of frontiers.' Article 19 of the Universal Declaration of Human Rights adds another important element, which is that this communication of opinions, information and ideas

[54] CJEU (Grand Chamber), 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12, pt. 68.

[55] CJEU (Grand Chamber), 24 September 2019, Google LLC, C-507/17.

[56] CJEU, 6 November 2003, Lindqvist, C-101/01.

can be done 'through any media.' Any direct attempt at cutting access to parts of the internet therefore appears to be a limitation of freedom of expression.

Furthermore, under the European Convention on Human Rights, states are also under certain positive obligations to ensure the respect of freedom of expression rights guaranteed under article 10 by private actors. Although there are not many cases where the ECtHR has found a violation of article 10 rights consecutive to the failure of a state to take action against a private person, it has reaffirmed the principle of the existence of positive obligations in several occasions.

Having established that universal access to a united internet derives from the fundamental right to the freedom of expression, any policy action aimed at undermining this unity is a limitation 'must be provided for by law and respect the essence of those rights and freedoms' and 'may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others' (art. 52 – 1 of the Charter of Fundamental Rights). In other words, and to use the vocabulary of the ECtHR, fragmentation is only legal if 'it is necessary in a democratic society.' Assessing whether a policy measure that acts as a factor of divergence is proportional may require conducting impact assessment of measures meant to apply to the internet, either as an infrastructure, a public sphere, a marketplace, or all of the previous. This has been supported by several interviewed experts, including David Frautschy, from the Internet Society.

Potential benefits

Establishing the unity of the internet as a fundamental digital right requires setting it, both legally and politically, at a higher level than laws and regulations in the hierarchy of norms. The inclusion of a statement on 'protecting a neutral and open internet where content, services, and applications are not unjustifiably blocked or degraded' in the proposed European Declaration on Digital Rights and Principles for the Digital Decade is therefore a step in the right direction.

A strategy based on recognising the unity of the internet as deriving from fundamental human right obligations of the EU does not mean that there are no limitations on that unity that can be justified and proportionate on grounds of public interest, including the need to establish a balance with other, conflicting fundamental right interests.

Policy options that are compatible with this strategy may include i.a.:

- Data localisation requirements and restrictions on data transfers. They can indeed be construed as limitations that are provided for by law, pursue legitimate public interests (privacy, data protection, protection of intellectual property rights, national security…), and appear to be proportionate given the fact that the CJEU has ruled that, in the field of data protection, it is an actual requirement deriving from article 8 of the Charter of Fundamental Rights on the right to the protection of personal data.
- Restrictions on certain technologies, such as the mining of crypto-currencies, may be justified on grounds of environmental protection.
- Information society service providers, including intermediaries, may be subject to certain rules to ensure that their decisions do not fragment the internet in a way that disproportionately affects fundamental rights. Indeed, in a societal context where some online platforms play a central role in the dissemination of information and in the economy, it is imperative that providers of information society services respect the fundamental rights of their users. Several provisions in the proposed DSA serve this purpose. It may even be argued that states are under positive obligations to ensure the protection of fundamental rights in the context of some private information society services, such as very large online platforms under the proposed DSA or gatekeepers under the proposed DMA. To use the words of Julia Pohle,

researcher at the Berlin Social Science Centre and internet governance expert, this can help integrate liberal logics into the network.
- Improving accessibility and interoperability requirements. This can help mitigate internet consolidation and reinforce resilience. It also helps combat walled gardens.

Interoperability is greatly helped by the existence and implementation of shared open standards. The EU can encourage the use of such standards. Art. 34 (1) of the proposed Digital Services Act contains wording to that effect, by stating that 'The Commission shall support and promote the development and implementation of voluntary industry standards set by relevant European and international standardisation bodies at least for' certain regulated activities, including 'interoperability of the advertisement repositories.'

Obligations stemming from the WTO's TBT Agreement limit the capacity of the EU or Member States to impose certain standards, but mechanisms can be introduced to ensure that actors are held accountable. Article 32 of the GDPR provides a good example of such a mechanism, by stating that 'taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.' The choice of the actual standard is in practice left to the choice of the data controller, which can still be held liable if it chooses to ignore appropriate global industry standards.

Potential Drawbacks and Legal Hurdles

Although fragmentation can be perceived as a path towards digital sovereignty, and is perceived as such by governments of countries such as China and Russia, experts such Rigo Wenning and Niels ten Oever, who both have extensive experience in internet technical standard-setting organisations, sovereignty would best be served by investing in the development of open source infrastructure and services that reduce dependence on foreign providers. The development of a European web browser has been suggested as something that would provide more leverage and influence in the field of internet governance. GAIA-X and DNS4EU are initiatives that have similar aims: developing strategic autonomy and European digital sovereignty by reducing dependency on foreign suppliers. However, proposals aiming at including technical elements that facilitate automated filtering of content present a risk as they may be misused in the long term.

6.3. Assessment of the policy options

The three first scenarios examined in this section appear to have significant drawbacks based on our assessment criteria: compatibility with international trade law, primary law and especially fundamental rights, or their capacity of maintaining the core architectural principles that allow the internet to function. However, the fourth scenario opens a new perspective for the EU in developing a consistent approach towards the topic of internet fragmentation.

The Open Internet Regulation provides that 'end-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service' (art. 3 of Regulation 2015/2120). This right can however be limited by other legislative acts and regulations and in practice by many different patterns of divergence, both at a technical level and in the content to be accessed. As evidenced by this report, this legislative text does not appear sufficient to provide for a consistent European approach towards the emerging public problem of internet fragmentation.

Framing the debate on internet fragmentation as a matter of fundamental rights comes with the advantage that human rights law is well equipped at dealing with the presence of conflicting rights and interests. This would allow the EU to develop a consistent policy, as presented in this report's conclusion. Instead of binary view on whether fragmentation is positive or detrimental as such, we construed it as a limitation to freedom of expression which can be proportionate and, to use wording used by the ECtHR, 'necessary in a democratic society.' This would for example cover requirements and limitations imposed on the transfer of personal data, while at the same time requiring the Commission to provide best efforts to reach adequacy decisions for all jurisdictions providing adequate protection of personal data.

A characteristic of the rule of law and of liberal democracies is the willingness of the state to limit its own power. Refraining from directly intervening in the structure of the infrastructure, especially if there is a risk it may lead to patterns of divergence in the online public sphere, could be construed as a mechanism of checks-and-balances in the digital era. This is without prejudice to the capacity of regulators and of the judiciary to hold actors of the internet ecosystem accountable for the design of their infrastructure and their choices of technical standards. It does not prevent the EU or its Member States from fixing certain objectives that public and private actors of the internet ecosystem are responsible for achieving using the best available practices, standards and protocols, developed through an open multi-stakeholder process.

Finally, although the scope of this report was centred on policy developments in the field of the Digital Single Market, it has to be pointed out that, especially in the current international context, it is also a relevant subject matter for EU foreign policy. Examining the example of the Global Online Freedom Act in the United States of America, and also private initiatives aimed at providing connectivity to countries with governments that censor access to the global internet, would be relevant to provide further policy options on a topic that deals with the governance of a global infrastructure and public sphere. The Global Gateway Initiative may also provide an opportunity to fund the development of an open, interoperable global digital infrastructure.

7. Conclusion

This report shows that there are many ways in which internet fragmentation can be defined. Fragmentation can be total or partial lack of connectivity, happen either at the transport or at the application layer, be caused by technical, commercial or political factors, and affect the internet either as a technical infrastructure, a digital public sphere, or both. This complexity explains the difficulty of formulating a strategy that approaches the topic in a consistent manner.

This report highlights how the fragmentation of the internet, and/or the desire to avoid it, will most likely be one of the issues around which the geopolitical and governance balances (of the internet, but not only) will be reconfigured in the near future, as demonstrated throughout the report, from the Cambodian kill-switch to Russia-China alignment in relation to internet governance.

The challenges raised by the intention of certain states to align internet infrastructure and content with their national interest raise the question of how to respond to those states that limit connectivity to limit key freedoms such as freedom of expression. As states are increasingly taking strategic approaches towards the internet and its standards, there appears to be a fine line between designing infrastructure that allows states to impose human rights-based values on the infrastructure through the use of territory-bounded legal instruments, and allowing the same infrastructure to function in a way in which internet users wanting to escape a walled-off internet imposed by human-rights-violating state actors remain able to do so.

Drawing on an analysis of recent patterns of internet fragmentation, differentiated in function of their underlying root causes, this report has explored the implications of the EU's recent policies in this field as well as the opportunities and challenges for EU Member States and institutions in addressing the so-called phenomenon of internet fragmentation. The report underlines how recent EU legislative proposals – on the Digital Services Act, Digital Markets Act, Artificial Intelligence Act, and NIS 2 Directive – have the potential to help address patterns of fragmentation. It also illustrates how their limitations and unintended consequences need to be addressed in order to ensure the coherence and consistency of the EU's action in this field.

In relation to these challenges, the EU legislative agenda can be seen as a driver for positive opportunities but also as a catalyst for the worsening of the very same threats. The EU digital single market strategy and the more recent 2030 'digital compass' both underline the EU's ambivalent commitment to promote the development of a single, open, neutral, free, secure and un-fragmented network, while adopting a more strategic approach to the process of developing internet standards and protocols.

Despite the existence of some policy initiatives aimed at strengthening a global and open internet, the European Union lacks a consistent strategy on the subject matter. This report explores four different scenarios: staying with the status-quo, embracing fragmentation, consistently resisting patterns of divergence or framing discussions as a matter of fundamental rights. This report underlines how the latter comes with the advantage of providing a framework based on proportionality and on the notion of checks-and-balances, which helps structure a consistent strategy that is compatible with international trade law as well as EU primary law, including human rights law.

References

Abbate, J., 'What and where is the Internet? (Re)defining Internet histories', *Internet Histories*, 1:1-2, 2017, 8-14, DOI: 10.1080/24701475.2017.1305836

Alvestrand, H. & Wium Lie, H., 'Development of Core Internet Standards: The Work of IETF and W3C' in Lee A. Bygrave and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions*. Oxford: Oxford University Press, 2009, pp. 126-146.

Alvestrand, H., A Mission Statement for the IETF. BCP 95, RFC 3935, October 2004.

Appelquist, D & Beeman, H., W3C TAG Ethical Web Principles. W3C TAG Finding, 06 October 2021. https://www.w3.org/2001/tag/doc/ethical-web-principles/

Apple, 'Prepare for removal of PPTP VPN before you upgrade to iOS 10 and macOS Sierra', 2018. Available at: https://support.apple.com/en-us/HT206844

Arkko, J. 'The influence of internet architecture on centralised versus distributed internet services', *Journal of Cyber Policy*, 5:1, 2020, 30-45.

Arkko, J., Trammell, B., Nottingham, M., Huitema, C., Thomson, M., Tantsura, J., & ten Oever, N., 'Considerations on internet consolidation and the internet architecture', *IETF Working Draft*, 2019.

Arsene, S., 'Internet domain names in China: Articulating local control with global connectivity'. *China Perspectives*, 4 (25), 2015, 25– 34.

Asmolov, G., & Kolozaridi, P., 'Run Runet runaway: The transformation of the Russian Internet as a cultural-historical object'. In *The Palgrave Handbook of Digital Russia Studies*, (pp. 277-296). Palgrave Macmillan, Cham, 2021.

Baran, P., 'On Distributed Communications: I. Introduction to Distributed Communications Networks'. RAND Corporation, 1964. https://www.rand.org/pubs/research_memoranda/RM3420.html (December 2, 2018).

Belli, L. 'Net neutrality, zero rating and the Minitelisation of the internet', *Journal of Cyber Policy*, 2:1, 2017, 96-122.

Berlin, I., 'Two concepts of liberty', In: *Four Essays on Liberty*, Oxford University Press, 118 – 172, 1969.

Bethell, O., 'Our commitments for the Privacy Sandbox', Google Blogpost, 11 Jun 2021. URL: https://blog.google/around-the-globe/google-europe/our-commitments-privacy-sandbox/

Bindra, C., 'Building a privacy-first future for web advertising', Google Blogpost, 25 Jan 2021.

Box, S. & West, J. K., 'Economic and Social Benefits of Internet Openness', *OECD Digital Economy Series* No. 257, June 22, 2016.

Bradford, A., 'The Brussels Effect', *Northwestern University School of Law*, 107, 1, 2012.

Broeders, D., *The public core of the internet*. Amsterdam: University Amsterdam Press, 2015.

Brown, I. (ed.), *Research Handbook on Governance of the Internet*. Cheltenham: Edward Elgar, 2013.

Bygrave, L., Schiavetta, S., Thunem, H., Lange, A. B., & Phillips, E. The naming game: governance of the Domain Name System. In L. Bygrave & J. Bing (Eds.), *Internet Governance: Infrastructure and Institutions* (pp. 147–212). Oxford: Oxford University Press, 2009.

Cath, C., & Floridi, L., The design of the internet's architecture by the Internet Engineering Task Force (IETF) and human rights. *Science and engineering ethics*, 23(2), 2017, 449-468.

Chenou, J-M., Radu, R., 'The 'Right to Be Forgotten': Negotiating Public and Private Ordering in the European Union', *Business & Society*, 58, 1, 74 – 102, 2019.

Claessen, E., 'Reshaping the internet–the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU'. *Journal of Cyber Policy*, 5(1), 2020, 140-157.

CNIL, 'Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply', 10 February 2022. Available at: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply.

Contreras, J. L., 'Divergent patterns of engagement in Internet standardization: Japan, Korea and China'. *Telecommunications Policy*, 38(10), 2014, 914-932.

Contreras, J., 'Patents and Internet Standards. Global Commission on Internet Governance'. *GCIG Paper Series*: n°29, 2016.

Cyphers, B., 'Don't Play in Google's Privacy Sandbox,' Electronic Frontier Foundation, August 30, 2019.

Dawit, B., A Partnership to Improve Africa's Internet Infrastructure Resilience and Reliability, Internet Society, Blogpost, 30 July 2020.

Deibert, R. J., & Crete-Nishihata, M., 'Global governance and the spread of cyberspace controls'. *Global Governance*, 18(3), 2012, 339-361.

Dell, P., 'On the dual-stacking transition to IPv6: A forlorn hope?'. Telecommunications Policy, 42(7), 2018, 575-581.

DeNardis, L., & Hackl, A. M., 'Internet governance by social media platforms'. *Telecommunications Policy*, 39(9), 2015, 761-770.

DeNardis, L., 'One Internet: an evidentiary basis for policy making on internet universality and fragmentation'. *CIGI*, n°38, 2016.

DeNardis, L., *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: MIT Press, 2009.

DeNardis, L., *The global war for Internet governance*. New Haven: Yale University Press, 2014.

Dönni, D., Machado, G., Tsiaras, C., Stiller, B., Schengen Routing: A Compliance Analysis. 9th Autonomous Infrastructure, Management, and Security (AIMS), Jun 2015, Ghent, Belgium. pp. 100-112, https://hal.archives-ouvertes.fr/hal-01410156

Doty, N., *Enacting Privacy in Internet Standards*. Doctoral dissertation. UC Berkeley. 2020.

Drake, W. J., Vinton, C. G., & Kleinwächter, W., 'Internet fragmentation: An overview'. World Economic Forum, 2016.

Dratwa, J. 'Analysing Community Policies', in: Henri Delanghe & Ugur Muldur & Luc Soete (ed.), *European Science and Technology Policy*, chapter 5, Edward Elgar Publishing, 2009.

Duerst, M., 'Internationalization of Domain Names', IETF, Internet Draft, June 1996.

Duke, M., 'QUIC will eat the Internet'. Blogpost, F5, 22 Feb 2021. URL: https://www.f5.com/fr_fr/company/blog/quic-will-eat-the-internet

Dumont, B., 'La régulation à l'échelle communautaire: Une analyse économique des instruments et institutions de la protection des données au sein de l'UE', *Réseaux*, 2011/3 n° 167, 2011, p. 49-73.

EDPB, 'Launch of coordinated enforcement on use of cloud by public sector', 15 February 2022. Available at: https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en

Ermoshina, K., & Musiani, F., 'Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era'. *Media and Communication*, 5(1), 2017, 42-53.

Ermoshina, K., & Musiani, F., 'The Telegram ban: How censorship 'made in Russia' faces a global Internet'. *First Monday*, 26(5), 2021.

Ermoshina, K., Loveluck, B., & Musiani, F., 'A market of black boxes: The political economy of Internet surveillance and censorship in Russia'. *Journal of Information Technology & Politics*, 1-16, 2021.

Facebook (2020) How Facebook is bringing QUIC to billions. Blogpost, October 21, 2020. URL: https://engineering.fb.com/2020/10/21/networking-traffic/how-facebook-is-bringing-quic-to-billions/.

Fragkouli, A., 'How Sanctions Affect the RIPE NCC', RIPE Labs, URL: https://labs.ripe.net/author/athina/how-sanctions-affect-the-ripe-ncc/, 18 Nov. 2021.

France 24, 'Cambodia sets up China-style internet firewall', 17 February 2022. Available at: https://www.france24.com/en/live-news/20210217-cambodia-sets-up-china-style-internet-firewall.

Galloway, A., *Protocol*. Boston: MIT Press, 2004.

Galloway, T. and Baogang, H., 'China and Technical Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance within ICANN, WSIS and the IGF', *China: An International Journal*, 12(3), 2014, 72–93.

Geradin, D. & Katsifis, D., 'An EU competition law analysis of online display advertising in the programmatic age', *European Competition Journal*, 15:1, 2019, 55-96.

Geradin, D., Katsifis, D. & Karanikioti, T., 'Google as a de facto privacy regulator: analysing the Privacy Sandbox from an antitrust perspective', *European Competition Journal*, 2021.

Greenstein, S., *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network*. Princeton, NJ: Princeton University Press, 2017.

Gusfield J.R., *The culture of public problems: drinking-driving and the Symbolic order*, Univ. of Chicago Press, 1994.

Harcourt, A., Christou, G. & Simpson, S., *Global Standard Setting in Internet Governance*. New York: Oxford University Press, 2020.

Hoffman-Andrews, J., 'ETS Isn't TLS and You Shouldn't Use It', EFF, March 2019. URL: https://www.eff.org/fr/deeplinks/2019/02/ets-isnt-tls-and-you-shouldnt-use-it.

Hoffmann, S., 'Understanding DNS over HTTPS – DoH'. Oxford Information Labs Blog. 19 August 2019. https://oxil.uk/blog/understanding-dns-over-https-doh/.

Hoffmann, S., Lazanski, D. & Taylor, E., 'Standardising the splinternet: how China's technical standards could fragment the internet', *Journal of Cyber Policy*, 5:2, 2020, 239-264.

Howell, D., 'HaDEA proposes DNS4EU, a secure DNS for EU member states', Neowin, 19 January 2022. Available at: https://www.neowin.net/news/hadea-proposes-dns4eu-a-secure-dns-for-eu-member-states/.

Huston, G., 'DNS resolver centrality'. Blogpost, APNIC, 23 Sep 2019. URL: https://blog.apnic.net/2019/09/23/dns-resolver-centrality/

ICANN, 'ICANN org comments on the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive (EU) 2016/1148 ('NIS2')', ICANN, 2021.

IDN World Report, 'Internationalised Domain Name World Report'. EURid, UNESCO and the Coordination Center for TLD.RU, 2019. Available at: https://idnworldreport.eu/archive/2019/.

IETF, 'A new era in Internet transport'. Blogpost, IETF, 3 Jun 2021. URL: https://www.ietf.org/blog/new-era-transport/.

IETF, 'QUIC in the Internet industry'. IETF News, 3 Jun 2021. URL: https://www.ietf.org/blog/quic-industry/.

IETF, 'RFC 8446, Transport Layer Security (TLS) Protocol Version 1.3'. Internet Engineering Task Force, August 2018.

ISC, 'DNS and Root Name Servers', Submission to the Public Consultation on the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive (EU) 2016/1148 ('NIS2'), Internet Systems Consortium Inc., March 2021.

Jobs, S., 'Thoughts on Flash', 2010. Available at: https://web.archive.org/web/20200430094807/https://www.apple.com/hotnews/thoughts-on-flash/.

Kamara, I. & Kosta, E., 'Do Not Track Initiatives: Regaining the Lost User Control'. *International Data Privacy Law*, 6(4), 2016, 276–90.

Keane, S., 'Mozilla engineer says Google slowed YouTube down on non-Chrome browsers', CNET, 2018, June 18. URL: https://www.cnet.com/tech/services-and-software/mozilla-exec-says-google-slowed-youtube-down-on-non-chrome-browsers/.

Kiernan, C. J. & Mueller, M. L., 'Standardizing Security: Surveillance, Human Rights, and the Battle Over Tls 1.3'. *Journal of Information Policy*, 11, 2021, 1-25.

Kim, M., Lee, H. & Kwak, J., 'The changing patterns of China's international standardization in ICT under techno-nationalism: A reflection through 5G standardization', *International Journal of Information Management*, 54, 2020.

Kolozaridi, P., & Muravyov, D., 'Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case'. *First Monday*, 2021.

Komaitis, K., 'GDPR: Going Beyond Borders', Internet Society, 25 May 2018. Available at: https://www.internetsociety.org/blog/2018/05/gdpr-going-beyond-borders/.

Kotaikis, K. 'The 'wicked problem' of data localisation', *Journal of Cyber Policy*, 2, 3, 355 – 365, 2017.

Kuerbis, B. & Mueller, M., 'The hidden standards war: economic factors affecting IPv6 deployment'. *Digital Policy, Regulation and Governance*, 2020.

Lambach, D. 'The Territorialization of Cyberspace', *International Studies Review*, Volume 22, Issue 3, 2020, 482–506.

Langheinrich, M., 'To FLoC or Not?', in IEEE Pervasive Computing, vol. 20, no. 2, pp. 4-6, 1 April-June 2021, doi: 10.1109/MPRV.2021.3076812.

Lemley, M. A., 'The Splinternet', *Duke Law Journal*, 70, 1397 – 1427, 2021.

Lessig, L., *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.

Levin, S. L. & Schmidt, S., 'IPv4 to IPv6: Challenges, solutions, and lessons'. *Telecommunications Policy*, 38(11), 2014, 1059-1068.

Lundqvist, B., *Standardization Under EU Competition Rules And US Antitrust Laws: The Rise and Limits of Self-Regulation*. Cheltenham: Edward Elgar, 2014.

McKelvey, F., *Internet Daemons. Digital Communications. Possessed*, Minneapolis: University of Minnesota Press, 2018.

Minoli, D., *Building the internet of things with IPv6 and MIPv6: the evolving world of M2M communications*. John Wiley & Sons, 2013.

Mueller, M. L., *Networks and states: The global politics of Internet governance*. MIT press, 2010.

Mueller, M., 'Against sovereignty in cyberspace', *International Studies Review*. volume 22, number 4, 2020, pp. 779–801. doi: https://doi.org/10.1093/isr/viz044.

Mueller, M., 'Internet Fragmentation Exists, But Not In the Way That You Think', Council on Foreign Relations, Blogpost, June 12, 2017. Available at: https://www.cfr.org/blog/internet-fragmentation-exists-not-way-you-think.

Mueller, M., *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press, 2004.

Mueller, M., *Will the Internet fragment? Sovereignty, Globalization, and Cyberspace*. Cambridge: Polity Press, 2017.

Musiani, F., 'Alternative technologies as alternative institutions: The case of the domain name system'. In: Musiani, F., Cogburn D. L., DeNardis L., Levinson N.S., *The turn to infrastructure in Internet governance*. Palgrave Macmillan, 73-86, 2016.

Musiani, F. & Schafer, V., 'Le modèle Internet en question (années 1970-2010)'. *Flux*, (3), 2011, 62-71.

Musiani, F., Cogburn, D. L., DeNardis, L. & Levinson, N. S., *The Turn to Infrastructure in Internet Governance*. Basingstoke: Palgrave Macmillan, 2016.

Musiani, F., New global top-level domain names: Europe, the challenger. *Internet Policy Review*, 2(2), 1-8, 2013.

Nanni, R., 'The 'China' question in mobile Internet standard-making: Insights from expert interviews'. Telecommunications Policy, 45(6), 2021.

Negro, G., 'A History of Chinese Global Internet Governance and Its Relations with ITU and ICANN'. *Chinese Journal of Communication* 13 (1), 2019, 1–18.

NetBlocks (a), 'Internet disruptions registered as Russia moves in on Ukraine', 24 February 2022. Available at: https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K

NetBlocks (b), 'Twitter and Facebook restricted in Russia amid conflict with Ukraine', 26 February 2022. Available at: https://netblocks.org/reports/twitter-and-facebook-restricted-in-russia-amid-conflict-with-ukraine-JBZrogB6.

Newman, A., *Protectors of Privacy, Regulating Personal Data in the Global Economy*, Ithaca: Cornell University Press, 2008.

Nix, N., 'Is Facebook Going to Have to Pull Out of Europe?', 10 February 2022. Available at: https://www.bloomberg.com/news/newsletters/2022-02-10/is-facebook-going-to-have-to-pull-out-of-europe.

Nocetti, J., 'Contest and conquest: Russia and global internet governance'. *International Affairs*, 91(1), 2015, 111-130.

Nottingham, M., 'Playing Fair in the Privacy Sandbox: Competition, Privacy and Interoperability Standards. Privacy and Interoperability Standards', February 3, 2021. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891335

Notthingham, M., 'Centralization and Internet Standards'. IETF, Network Working Group, 9 February 2022. URL: https://www.ietf.org/archive/id/draft-nottingham-avoiding-internet-centralization-02.html.

NOYB, 'Austrian DSB: Use of Google Analytics violates 'Schrems II' decision by CJEU', 13 January 2022. Available at: https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal.

O'Neill, M., 'Do Not Track and the GDPR', W3C Blog, 2018. URL: https://www.w3.org/blog/2018/06/do-not-track-and-the-gdpr/.

Papastergiou, G., Fairhurst, G., Ros, D., Brunstrom, A., Grinnemo, K. J., Hurtig, P., ... & Mangiante, S., 'De-ossifying the internet transport layer: A survey and future perspectives'. *IEEE Communications Surveys & Tutorials*, 19(1), 2016, 619-639.

Peng, S., 'Private Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime'. *Cornell International Law Journal*, 51(2), 2018, pp. 445-469.

Perarnaud, C., 'A step back to look ahead: mapping coalitions on data flows and platform regulation in the Council of the EU (2016-2019)'. *Internet Policy Review*, 10(2), 2021.

Pigman, L., 'Russia's vision of cyberspace: A danger to regime security, public safety, and societal norms and cohesion', *Journal of Cyber Policy*, volume 4, number 1, 2019, pp. 22–34.

Poell, T. & Nieborg, D. & van Dijck, J., 'Platformisation'. *Internet Policy Review*, 8(4), 2017.

Radu, R & Hausding, M., 'Consolidation in the DNS resolver market – how much, how fast, how dangerous?', *Journal of Cyber Policy*, 5:1, 2020, 46-64.

Radu, R., Kettemann, M., Meyer, T. & Shahin, J., 'Normfare: Norm entrepreneurship in internet governance'. *Telecommunications Policy* 45:6, 2021, pages 102148.

Radu, R., *Negotiating Internet Governance*. Oxford: Oxford University Press, 2019.

Riley, C., 'Unpacking interoperability in competition', *Journal of Cyber Policy*, 5:1, 2020, 94-106.

Roberts, J. J., 'The GDPR and Our Balkanized Internet', Fortune, 26 May 2018. Available at: https://fortune.com/2018/05/26/gdpr-internet/.

Rossi, J., 'What rules the Internet? A study of the troubled relation between Web standards and legal instruments in the field of privacy'. *Telecommunications Policy*, 45(6), 2021, 102143.

Russell, A. L., 'The W3C and Its Patent Policy Controversy: A Case Study of Authority and Legitimacy in Internet Governance', August 31, 2003. TPRC 2003. Available at SSRN: https://ssrn.com/abstract=2056900.

Sabatier, P. A., & Jenkins-Smith, H. C. (eds.), *Policy Change and Learning: An Advocacy Coalition Approach*. Boulder, Colo: Westview Press, 1993.

Schuh, J., 'Building a more private web: A path towards making third party cookies obsolete', Chromium Blogpost, 14 Jan 2020. URL: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html.

Seaman, J., 'China and the New Geopolitics of Technical Standardization', *Notes de l'Ifri*, Ifri, January 2020.

Sharp, H., & Kolkman, O., 'Discussion Paper: An analysis of the' New IP' proposal to the ITU-T'. Internet Society, 2020. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/ISOC-Discussion-Paper-NewIP-analysis-24April2020.pdf.

Shen, H., 'Building a digital silk road? Situating the internet in China's belt and road initiative'. *International Journal of Communication*, 12, 19, 2018.

Shen, H., 'China and Global Internet Governance: Toward an 'Alternative Analytical Framework'', *Chinese Journal of Communication* 9 (3), 2016, pp. 304–324.

Simcoe, T. & Watson, J., 'Forking, Fragmentation, and Splintering', *Strategy Science*, INFORMS, vol. 4(4), 2019, pp. 283-297.

Smolenskiy, M. and Levshin, N. 'GDPR Implementation as the Main Reason for the Regional Fragmentation in the Online Mediasphere', *E3S Web of Conferences* 273: 08099, 2021.

Souter, D., & Van der Spuy, A., UNESCO's Internet Universality Indicators: A Framework for Assessing Internet Development. UNESCO, 2019.

Stadnik, I., 'Control by infrastructure: Political ambitions meet technical implementations in RuNet'. *First Monday*, 26(5), 2021.

Taylor, E.& Hakmeh, J. (eds.) 'Special Issue: Consolidation of the Internet'. *Journal of Cyber Policy*. Taylor & Francis 5 (1), 2020.

ten Oever, N., *Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure*. Ph.D thesis, University of Amsterdam, 2020.

Tréguer, F., *L'utopie déchue*. Paris: Fayard, 2019.

UK's Competition and Markets Authority, 'Online platforms and digital advertising market study'. CMA, London, 2020. URL: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

Vale, M., 'Privacy, sustainability and the importance of 'and'', Google Blogpost, 30 Mar 2021. URL: https://blog.google/products/chrome/privacy-sustainability-and-the-importance-of-and/.

Veale, M. & Zuiderveen Borgesius, F., 'Adtech and Real-Time Bidding under European Data Protection Law', *German Law Journal*, 2021.

Vezzoso, S., 'Android and Forking Restrictions: On the Hidden Closedness of 'Open'. *Market and Competition Law Review*, (2018).

Vialle, P., Song, J., & Zhang, J., 'Competing with dominant global standards in a catching-up context. The case of mobile standards in China'. *Telecommunications Policy*, 36(10-11), 2012, 832-846.

Weyrauch, D., & Winzen, T., 'Internet fragmentation, political structuring, and organizational concentration in transnational engineering networks'. *Global Policy*, 12(1), 2021, 51-65.

Wijermars, M., 'Selling internet control: the framing of the Russian ban of messaging app Telegram'. *Information, Communication & Society*, 2021, 1-17.

Zalnieriute, M., & Milan, S., 'Internet architecture and human rights: Beyond the human rights gap', *Policy & Internet*, 2019.

Zittrain, J., ''Don't Force Google to 'Forget'', New York Times, Opinion, 14 May 2014. Available at: https://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html.

Zittrain, J., *The future of the Internet—And how to stop it*. New Haven: Yale University Press, 2008.

Appendices

A1. Technologies and protocols under study and their role in internet divergence and convergence.

Technologies/Protocols	Implications
Deployment of IPv6	Technical splintering
Concurrent deployment of TLS 1.3 and ETS	Technical splintering
Establishment of a hegemonic position for one or a few web browser engines	Technical splintering
Development of 'sovereign'/national DNS and Internet architecture	Technical splintering
Lack of universal acceptance for internationalised domain names	Technical splintering
(Planned) obsolescence of technologies and protocols	Technical splintering
Ubiquity of middleboxes (NAPTs, firewalls)	Internet ossification
Adoption of QUIC	Internet consolidation
Concentration of DNS resolution services	Internet consolidation
Deployment of FLoC and Topics API	Internet consolidation

A2. Key organisations in the development of a selection of Internet standards and protocols.

TCP/IP Layer	Standards	SDOs/Organisations
Application	HTTP, HTML, CSS HTTP, HTML, IMAP, POP XML	W3C IETF OASIS
Transport	TCP, UDP, SSL, TLS, QUIC ETS	IETF ETSI
Internet	IPv4, IPv6	IETF
Network	WiFi, Ethernet, IoT IoT, 5G 5G 5G	IEEE ITU-T ETSI 3GPP

A3. EU legislative dossiers under study and their relevance to Internet fragmentation.

Legislative dossiers	Implications for Internet fragmentation
Artificial Intelligence Act 2021/0106(COD)	- The territorial scope of the proposed act implies that technology providers will need to comply with EU requirements, or choose not to, leading thus to a possible splintering in the type of services and applications for users outside of the EU. - The proposal adopts an approach to self-assessment and standardisation that could risk absolving public authorities from policymaking, and offloading it to privatised standards fora.
Digital Markets Act 2020/0374(COD)	- The proposed legislative text introduces new obligations related to access, installation, portability and interoperability for large Internet platforms. - It could limit the ossification of gatekeepers' services and support more competition in the digital economy. - The legislation could prohibit the introduction by national authorities of more stringent obligations for gatekeepers in terms of interoperability requirements. - The current text stops short of providing full support for device-neutrality as it gives manufacturers to sell hardware bundled with the operating system, without giving the user any choice or transparency on the compatibility with competing operating systems.
Digital Services Act 2020/0361(COD)	- The DSA introduces a right for users to learn about the main parameters used in recommender systems and a right to opt for a system that is not based on profiling. - The proposed text may introduce new obligations for DNS services. - The proposed text calls for the development and implementation of voluntary industry standards, as opposed to standards defined as part of transparent, multistakeholder and inclusive processes. - The proposed text does not introduce minimum interoperability requirements for very large online platforms. - The negotiations could lead to changes of one of the core principles of the 2001 e-Commerce Directive, namely the country of origin principle, and thus have a significant impact on the way take-down orders are enforced globally.
NIS 2 Directive 2020/0359(COD)	- The revised NIS Directive could apply to all DNS service providers, considered as essential services, including recursive resolvers and operators of authoritative servers for the root zone, top-level domains (TLDs), and all other domain names below the TLDs. - If reciprocated by other foreign governments, these regulatory requirements could significantly complicate the operation of a fundamental component of the Internet's global infrastructure.

Recent events have multiplied concerns about potential fragmentation of the internet into a multitude of non-interoperable and disconnected 'splinternets'. Composed of thousands of compatible autonomous systems, the internet is by definition technically divided. Yet, the internet was also designed to be an open and global technical infrastructure. The unity and openness of the internet appear to be under great pressure from political, commercial and technological developments.

This report explores the implications of the EU's recent policies in this field as well as the opportunities and challenges for EU Member States and institutions in addressing internet fragmentation. It underlines how recent EU legislative proposals – on the digital services act, digital markets act, artificial intelligence act, and NIS 2 Directive – could help to address patterns of fragmentation, but also have limitations and potentially unintended consequences.

Four possible strategies emerge: stay with the status quo, embrace fragmentation, resist patterns of divergence, or frame discussions as a matter of fundamental rights.

QA-09-22-292-EN-N

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service

ISBN 978-92-846-9621-5 | doi:10.2861/183513 | QA-09-22-292-EN-N