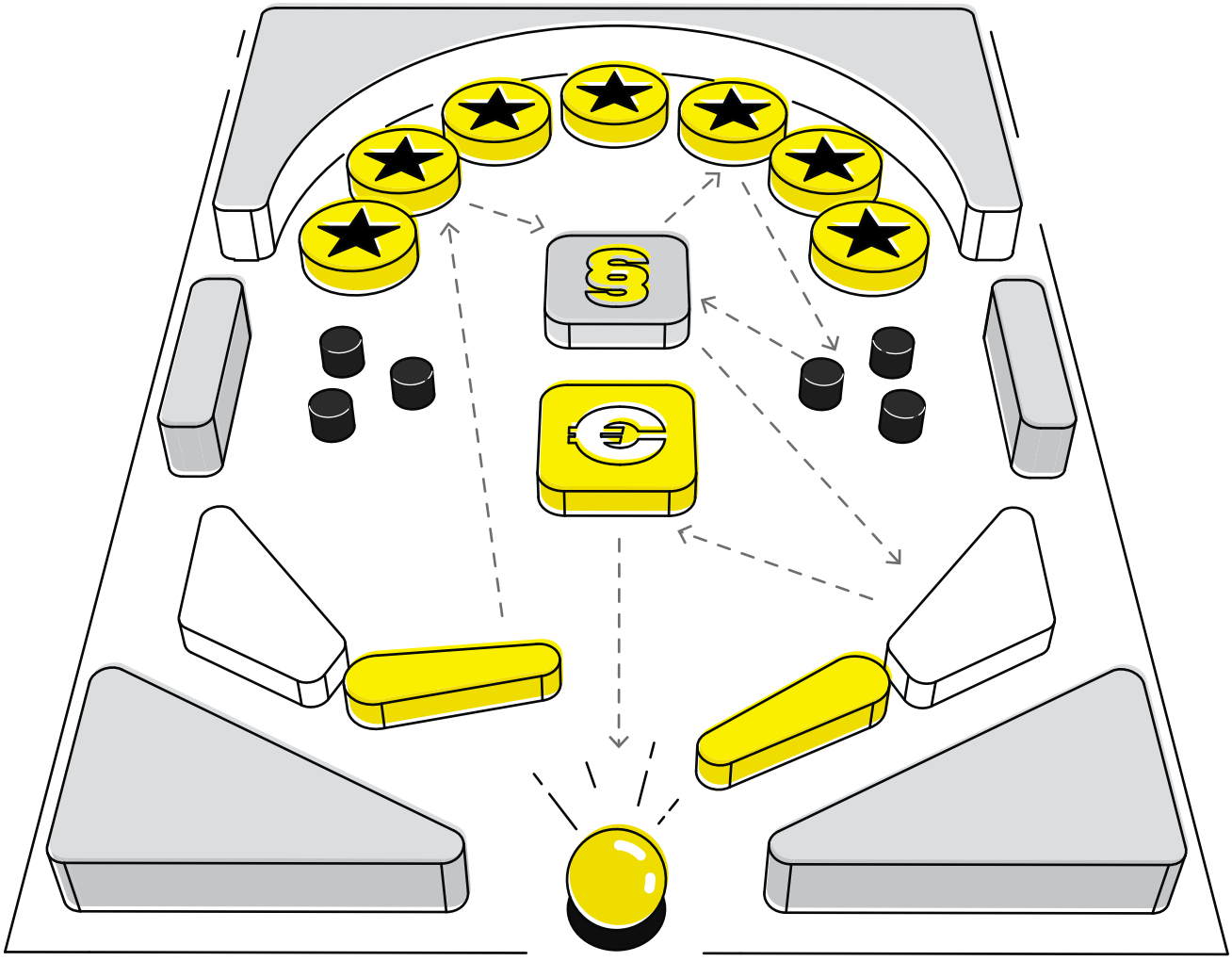
FINDING THE PATH TO A MORE OPEN INTERNET

a new European approach towards internet standards



OPEN _FUTURE

FEBRUARY 2024

Clément Perarnaud

ABSTRACT

This report aims to frame a new vision for what could become the future of the European Union's (EU) Open Internet agenda, as part of the next European Commission's mandate in 2024. Though also acknowledging recent positive steps, this report challenges the consistency of the European approach toward Open Internet standards and identifies a series of legislations and initiatives that seemingly contradict the overall stance of the EU in favor of protecting the internet as a global, interoperable, and open network of networks. The report identifies what could be the main building blocks for a renewed EU approach in view of remediating those inconsistencies. It lists six specific areas in which the EU could support the development of more "open" internet standards, referring both to the standards themselves and to the processes by which they are formulated and adopted. These recommendations are expected to pave the way for an alternative path for upcoming EU digital policies, conducive to more openness for the future of the internet.

INTRODUCTION

The internet is often celebrated for its openness. Usually presented as one of the few critical properties having propelled the internet's success over recent decades, the notion of openness remains at the heart of its founding mythology.[1]

Though for arguably different reasons, the openness of the internet is supported by a wide range of civil society organizations, companies, and states, using this concept as a synonym for "free," "interoperable," or "market-friendly."

Despite all of its supporters, there is an emerging consensus that the Open Internet is now under threat. Two major developments are generally considered, namely the almost unparalleled power gained by a few technological monopolies over the internet, and the acceleration of the assertiveness of state actors in relation to its infrastructure and governance. In part justified by the former, the growing assertiveness of states is evidenced by new claims supporting the protection of their digital sovereignty. Though there are of course different understandings of what it means in practice, the concept of digital sovereignty generally refers to the ambition that states and governments should reaffirm their authority and protect their self-determination in the digital sphere.[2] Such claims are generally voiced as an alternative to a "hegemonic" status quo,[3] at times identified as the ever-growing power of Big Tech, and/or the broader dominance of powerful states such as the U.S. or China over the internet.

---

[1] Russell, Andrew L. Open Standards and the Digital Age. Cambridge University Press, 2014.

[2] Musiani, Francesca. "Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices." Information, Communication & Society 25, no. 6 (2022): 785-800.

[3] Couture, Stephane, and Sophie Toupin. "What does the notion of 'sovereignty' mean when referring to the digital?" New Media & Society 21, no. 10 (2019): 2305-2322.

While India, Russia, and China have been actively developing their own sovereign internet infrastructures[4] over recent years, the EU has also become a strong advocate of its own declination of digital sovereignty, and notably since the beginning of the Commission's von der Leyen presidency in 2019.

Departing from its traditional market-driven approach applied to digital policies,[5] this shift has led to forceful attempts to curb the power of large technological companies over European digital markets, but also to increase the EU's influence over global internet standard-setting processes, as will be investigated throughout this report.

Standards are indeed at the center of many states' and companies' strategies to exert global influence and shape the internet "in their own image."[6] Standards allow for the interoperability between the tens of thousands of autonomous systems connecting worldwide. Standards have become arguably the most important pieces of the infrastructure making the internet a global network of networks. Due to their economic and strategic importance, internet standards are thus inevitably the subject and reflection of intense economic and political battles.

This report studies the implications of having an EU policy agenda characterized by new sovereignty claims in this domain and explores the specific case of internet standardization. Identifying clear inconsistencies between the EU's aspiration to promote Open Internet standards and its most recent digital policy trajectory, the report proposes a series of avenues to develop a renewed EU vision conducive to more openness for the internet.

The remainder of the report is structured as follows. The next section provides an analysis of the EU's approach toward internet standards in the context of its recent policy agenda centered since 2019 around the notion of digital sovereignty. After challenging the trajectory and consistency of its policies, the report identifies what could be the main building blocks for a renewed EU approach fostering more openness in the field of internet standardization.

---

[4] Nanni, Riccardo. "Digital sovereignty and Internet standards: normative implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force." Information, Communication & Society 25, no. 16 (2022): 2342-2362.

[5] Seidl, Timo, and Luuk Schmitz. "Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy." Journal of European Public Policy (2023): 1-28.

[6] Broeders, Dennis. The public core of the internet: An international agenda for internet governance. Amsterdam University Press, 2016.

UNPACKING THE EU'S APPROACH TOWARD INTERNET STANDARDS: WHEN DIGITAL SOVEREIGNTY MEETS THE OPEN INTERNET

In her State of the Union Address in 2020, the European Commission president Ursula von der Leyen emphatically voiced the EU's objective to "secure [its] digital sovereignty" and "lead the way on digital – or it will have to follow the way of others, who are setting these standards for us." Those words illustrate the clear process of "geopoliticization" of EU digital policies[7] that could be observed under her presidency, bringing digital issues in the remits of geopolitical competition.

In 2022, the European Commissioner Thierry Breton illustrated this new geopolitical European approach to standardization by stating that: "In French we say 'qui fait la norme, détient le marché': 'who makes the standard holds the market.' [...] If we want to ensure Europe's technological sovereignty in crucial disruptive sectors such as 5G, batteries, hydrogen or quantum technology, we must occupy the field of standard-setting. We must become standard-makers, and not just standard-takers."

This discourse, followed by many others, also underlined that the rationale for the EU approach has been primarily defensive ("defend the open, decentralized internet") and framed as a reaction to two main developments. First, EU discourses on internet standards usually factor proposals voiced by Chinese entities to transform core protocols on which the internet relies, initiatives that are part of a broader impetus from China to gain power through international standardization. But if China is now considered as an emerging security and strategic challenge for the EU, as highlighted by the adoption of the EU toolbox for 5G security in 2020, it is not the only justification for a stronger EU policy agenda in this area. The EU approach also identifies the dominance of large U.S.-based technological companies on digital markets as a clear policy issue. It justified the adoption of a brand new repertoire of legislative measures, such as the 2022 Digital Markets Act (DMA), as well as other lesser-known initiatives with equally important impacts on internet standards, detailed below.

Thus, the policy narrative of the European Commission clearly emphasized the need for the EU to set global standards in order to achieve its own digital sovereignty. Though it is difficult to characterize the EU approach to digital sovereignty, it is usually qualified[8] as the EU's attempt to regain control over the digital field and develop international leadership capacity. In this context, an over-reliance on standards set outside of the European continent is presented as clashing with the protection of a global, open, free, and decentralized internet, in stark contrast

[7] Broeders, Dennis, Fabio Cristiano, and Monica Kaminska. "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions." JCMS: Journal of Common Market Studies 61, no. 5 (2023): 1261–80.

[8] Bellanova, Rocco, Helena Carrapico, and Denis Duez. "Digital/sovereignty and European security integration: an introduction." European Security 31, no. 3 (2022): 337-355.

with other state actors such as Russia and China, treating digital sovereignty as equivalent to territorial sovereignty[9] over the internet.

This discursive connection between standards and digital sovereignty in the European policy agenda has materialized in a number of areas and through different instruments. The following section presents the most relevant EU initiatives adopted between 2019 and 2023.[10] It also discusses the coherence and consistency of the overall EU approach in relation to the protection of the internet's openness.

EU standardization strategy and digital policies

Over recent years, the EU has been particularly active in the digital policy space, with direct implications for internet standards. This is primarily illustrated by the 2022 European standardization strategy but also by other digital policy legislations such as the Digital Markets Act and the eIDAS regulation.

In contrast with its predecessor, the 2022 EU standardization strategy explicitly identifies internet standardization as a key area of interest. It states that "a particularly critical situation relates to internet standardization to promote a free, open, accessible, inclusive and secure global Internet" and warns about the increasing politicization of "the international standardisation [of] Internet protocols," which could limit "the evolution of the global open Internet."

One of the pillars of the strategy focuses on coordination between EU institutions and European Member States, emphasizing the need to "strengthen the EU's voice in global standardisation." This part is reflective of the fact that currently, "EU Member States allocate varying amounts of resources to the international standardisation bodies, and the European Union as such does not have a formal voice in multilateral fora."

This applies both to international standard-developing organizations (SDOs), such as the Internet Engineering Task Force (IETF), as well as European standardization organizations (ESOs), as underlined in the next paragraph.

As the only organizations eligible to work on standardization requests from the European Commission, we know that the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN), and the European Committee for Electrotechnical Standardization (CENELEC) are increasingly visible, as a result of their important role in the implementation phase of recent and upcoming EU digital legislations (such as the AI Act). Due to their significant importance, the 2022 standardization strategy indicates the intention of the European executive to restructure the decision-making process of these European SDOs, and, in particular, ETSI. Indeed, the Commission had recently expressed

[9] ibid.

[10] This section partly draws on a recent academic publication, co-authored with Dr. Julien Rossi, investigating the interplay between the EU and internet standards.

concerns that ETSI's decision-making system granted a disproportionate voting power to "certain corporate interests." Huawei is, for instance, a founding member of ETSI's Industry Specification Group on Securing Artificial Intelligence.

Despite its ESO status, the Commission argued that ETSI's governance and membership cannot be understood as strictly European. Based on this approach, the recent adoption of a targeted amendment to Regulation 1025/2012 on European standardization stated that for an ESO to be eligible for standardzation requests from the Commission, its internal governance must ensure that the national standardization bodies of European countries will "hold the decision-making power in each stage of the development of a standard requested."[11] This means the decision-making process of ETSI, which generally consisted of giving one vote per company (regardless of where it is headquartered), would have to change when dealing with standards requested by the Commission. This evolution challenges, to a certain extent, the scope and raison d'être of ETSI, which had projected itself over the years as a global SDO, rather than an European one.

This particular focus on ETSI could suggest that the influence of foreign companies in CEN-CENELEC is less of a challenge. Yet, non-EU companies are often active directly at the level of national standardization bodies, and their views thus get to be represented regularly at the European level through CEN-CENELEC, though via more indirect means.

The EU standardization strategy may have direct implications for the process of making internet standards, as ETSI has historically been a major actor in the field of mobile internet standards, but also at the transport layer of the internet in the development of new encryption protocols. From this standpoint, the strategy seems to conflict with the broader policy discourse of the EU regarding the global and open internet, as it seemingly pushes in favor of a regionalization of technological standardization that could affect internet infrastructures.

While these recent attempts by the Commission could create momentum in support of a form of regionalization of global standardization, the inherent contradictions of the EU approach underline, however, the limited capacity of the EU to isolate itself from global standardization processes. First, recent changes in ETSI's leadership are not really indicative of a new trajectory, as a representative from the U.S. company Intel has become ETSI's chair in December 2023. In addition, it should be noted that many European standards – including harmonized standards – directly refer to specifications from global, and arguably U.S.-led, consortia, underlying the great reliance of the European standardization system on global private SDOs to develop state-of-the-art specifications.

Aside from the standardization strategy, the EU has adopted a few important legislations with direct implications for internet standards and internet SDOs. The first is the 2022 Digital Markets Act (DMA), one of the flagship initiatives of the EU to curb the monopoly powers of Big Tech actors (labeled as "gatekeepers") in European digital markets. In this context, the DMA requires interoperability between message services from the most used messaging apps, such as Meta's

[11] The Commission expects this measure to grant more power to European actors in ESOs, and particularly within ETSI, where the national delegation principle does not apply.

Messenger or WhatsApp. Though not formally requested as such by the European Commission, the actual standardization of an interoperable protocol has been initiated by a few actors of this industry in the IETF in 2022 as part of the MIMI working group. This example illustrates a little-known channel through which the EU digital sovereignty agenda is directly influencing the internet standardization field. It is an important case of an EU sovereignty-oriented legislation directly affecting the work of the IETF, a traditionally industry-driven organization with a global reach.

In another important EU legislation, the eIDAS regulation, discussions about EU-approved certificate authorities for web browsers have been on the policy agenda. This followed a proposal by the European Commission to force web browsers to approve government-approved qualified website authentication certificates (QWACs), rather than preserving their freedom as to which certificates they could recognize as secure to protect communications. Justified by cybersecurity goals, this initiative has been challenged[12] by both the technical community and civil society organizations due to the political implications of this change for privacy, notably because it could allow third parties to intercept and modify traffic without the knowledge or consent of the sender and recipient.[13] Though the compromise adopted in trilogues in November 2023 eventually states that "the requirement to QWACs does not affect browser security policies," it signals another clear attempt by the EU to alter internet standards on the grounds of protecting its digital sovereignty.

EU research and innovation projects

Besides legislations, the EU approach in relation to internet standards has also taken the form of a series of research and innovation projects. Some can be framed as additional concretizations of the EU digital sovereignty agenda.

The European Commission has, for instance, identified a set of specific internet standards, understood as the right vehicles for protecting the Open Internet through its new EU Internet Standards Deployment Monitoring Website. This monitoring website provides deployment indicators of 18 key internet standards that will "help to secure the Internet and support its constant technological evolution." This tool is purely descriptive, but shows the priority given by the Commission toward five categories of standards: 1. Browsing – Web communication standards, 2. Routing – Mutually Agreed Norms for Routing Security (MANRS), 3. Emailing – Email communication security standards, 4. Naming – Domain Name System Security Extensions (DNSSEC), and 5. Addressing – Internet Protocol version 6 (IPv6).

In parallel, StandICT, a recent EU-funded project launched in 2018, has aimed to increase European experts' presence in international standardization in the broad field of ICT. It addresses

[12] Internet Society. "Internet Impact Brief: Mandated Browser Root Certificates in the European Union's eIDAS Regulation on the Internet."

[13] Other important legislations, such as the Cyber Resilience Act and the Artificial Intelligence Act, also have a number of implications for technological standard-setting, but they remain out of the scope of this report, which is focused on internet standards per se. For more see: https://www.ceps.eu/with-the-ai-act-we-need-to-mind-the-standards-gap/.

the fact that funding can be an important barrier to participation for individuals and small companies (along with technical expertise or language). This project is now considering internet standardization as a priority, in view to add more European voices to internet SDOs. Up until now, this funding stream had rarely benefited IETF participants, but there is now an intention to address this issue.

Finally, another important EU-funded project is the DNS4EU initiative. It is not strictly focused on internet standardization as such, but still refers to a number of key objectives related to internet standards. Featured in the 2020 EU Cybersecurity Strategy for the Digital Decade, this initiative has the ambition to develop a public European Domain Name System (DNS) resolver service. The function of a DNS resolver is to "resolve" the queries of users when they connect to a website, by translating domain names into IP addresses. The DNS resolver market is known for its rapid concentration, leading a handful of companies – based mostly outside of the EU – to control a significant portion of the internet traffic.

Though the initial intention to deconsolidate the market of DNS resolvers is laudable, this project reveals a number of inconsistencies in the EU approach. Though it has been introduced on the grounds of increasing cybersecurity and privacy protection, as well as avoiding an over-reliance on the solutions provided by U.S.-based companies (Google in the first place), it could nonetheless create a worrying precedent. Indeed, while it intends to contribute to the normalization of privacy-protecting protocols developed by the internet community (including the IETF), it is at the same time providing pathways and normalizing discourses for state actors to directly intervene in the internet architecture.[14] Despite of its potential implications, it should be acknowledged that the actual realization of this new DNS resolver appears to be, to this day, at a standstill.

International cooperation and technological diplomacy

Aside from these research and innovation projects, the EU has been active in relation to internet standards through a myriad of initiatives and collaborations carried out with third countries. The 2021 EU Global Gateway initiative – which mirrors the approach of the Chinese Belt and Road Initiative (BRI) and its Digital Silk Road – is one of them. The EU Global Gateway is expected[15] to link investments into technological infrastructure with the deployment of standards and rules in third countries. The Commission has explicitly stated that investments in digital infrastructure will be "linked with standards and protocols that support network security and resilience, interoperability, and an open, plural and secure Internet." Though the actual concretizations of this initiative remain limited so far in the area of digital infrastructure, this initiative shows that, conceptually, the deployment of certain internet standards is now being advanced through digital infrastructure investments in developing countries (now framed as "partner countries" in EU jargon).

---

[14] Perarnaud, Clément, and Julien Rossi. "The EU and Internet standards–Beyond the spin, a strategic turn?" Journal of European Public Policy (2023): 1-25.

[15] Karjalainen, Tyyne. "European Norms Trap? EU Connectivity Policies and the Case of the Global Gateway." East Asia (2023): 1-24.

The launch of the EU-US Trade and Technology Council (TTC) in 2021 also suggests evolutions in the EU approach. Though its mandate is broader, this transatlantic mechanism is expected to promote the alignment of EU-U.S. positions within international standard-setting bodies, including internet SDOs, and for instance through the new Strategic Standards Information mechanism. Once again, the actual outcome of this new cooperation stream remains to be seen, but it nonetheless echoes the growing geopolitical nature of internet standards for the EU.

Finally, the European Commission, through DG CONNECT and DG INTPA, has also initiated a series of lobbying and public relation campaigns toward third countries focusing on internet standards. The EU is attempting to engage with specific countries,[16] mostly on the African continent, in view of upcoming ITU plenaries – the prime objective being to counter the growing influence of China in this fora.

The recent European Commission's international approach toward internet standards is thus much more geopolitical than in the past. At the same time, attempts to enhance the EU's digital sovereignty create clear frictions with the European vision favoring the promotion of an Open Internet.

If defending the internet's openness was and remains a common denominator at the European level, this report points to a series of inconsistencies, some of which are highlighted in the following table, questioning the coherence of the EU's policy approach.

[16] Perarnaud, Clement, and Julien Rossi. "The EU and Internet standards–Beyond the spin, a strategic turn?" Journal of European Public Policy (2023): 1-25.

TYPE	INITIATIVE	KEY IMPACTS ON INTERNET STANDARDS
EU legislation and policy strategy	2022 standardization strategy	push in favor of a regionalization of technological standardization, that could affect internet infrastructures
	Digital Markets Act (DMA)	introduce interoperability provision directly influencing the work of the IETF
	eIDAS regulation	proposal of EU-approved certificate authorities for web browsers could allow third parties to intercept and modify traffic
EU research & innovation projects	Internet Standards Deployment Monitoring	provide descriptive deployment indicators of 18 key internet standards
	StandICT	support increase of European experts' presence in international standardization
	DNS4EU	create a new public DNS resolver, but also provide pathways and normalize discourses for state actors to directly intervene in the internet architecture
International tech diplomacy and global cooperation	Global Gateway	support the deployment of certain internet standards through digital infrastructure investments in developing countries
	EU-US TTC	promote the alignment of EU-U.S. positions within international standard-setting bodies, including internet SDOs
	ITU diplomacy	counter the growing influence of China in the ITU through influence campaigns

This diverse set of initiatives highlights the way in which the EU policy agenda has been shaped by new sovereignty claims in this domain, with admittedly varying levels of ambition and success. It also appears clear that, while certain attempts provide for useful policy gestures, others may be seen as incompatible with the broader public policy message of the EU in relation to the open and global internet. This is especially problematic as today's internet is already known to be characterized by a series of patterns that gradually limit its openness. They include the consolidation of its infrastructures in the hands of a small set of companies, the various claims for more network control expressed by states, and the privatization of decision-making in relation to global internet standards.

In response to these challenges and inconsistencies, the following section lays down the building blocks of what could be a new European vision conducive to more openness in relation to the internet.

BUILDING BLOCKS FOR A NEW EUROPEAN APPROACH TOWARD OPEN INTERNET STANDARDS

It is commonly admitted that the policy approach of the EU in relation to the digital economy, and more broadly to the internet, can have a great impact worldwide. The much-commented on "Brussels Effect" popularized by Anu Bradford[17] is a testimony to the fact that EU norms can have a significant influence well beyond European borders, in part due to the still significant economic power of its market.

With its new agenda promoting digital sovereignty, we have shown how the EU is normalizing a set of discourses and technical interventions related to the internet that can be construed as a challenge to its openness. Though in different ways, this is illustrated by recent initiatives and projects such as the DNS4EU, the eIDAS, or the EU standardization strategy.

Having identified areas in which the EU policy approach generates inconsistencies, we now reflect on avenues for the next European Commission to reimagine its approach in the near future. The report identifies six areas in which the EU could support the development of more open internet standards, referring both to the standards themselves and to the processes by which they are formulated and adopted. The first part reflects on what should be the role – and even responsibility – of the EU in promoting certain types of internet standards. The second focuses on how to better reflect the public interest in private standardization processes.

Supporting standards conducive to more internet openness

As exemplified by the 2022 EU standardization strategy or the EU Global Gateway initiative, the Commission has recently developed a series of channels by which it aims to support the deployment of certain standards across the EU and abroad. In this context, specific internet standards are being supported by the European Commission at technical and political levels.

It is currently unclear what the criteria are on which the current selection of standards is based, besides fostering the growth of the network and its security. Though these objectives are entirely legitimate, this report argues that the EU would gain from prioritizing a broader set of policy objectives, and thus a more diverse range of standards. This should be done through the various ways in which the EU can promote the deployment of internet standards, considering for instance public procurements and investments in digital infrastructure.

As fostering interconnectivity should not be an end for itself, one would need to make sure that the internet standards supported by the EU are aligned with the overarching goal of the development of an open, people-centered internet. EU-supported internet standards need to have broader objectives, including to foster the de-consolidation of the internet, push for greater cooperativity, and support, unequivocally, end users' privacy. These objectives could be

[17] Bradford, Anu. The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020.

operationalized through the various means currently at the disposal of the EU, including public procurements, and as part of a dedicated strategy on internet standardization.

A. DE-CONSOLIDATING THE INTERNET

If it was to convert its internal digital competition policy into action on the global standardization front, the EU could support the formulation and deployment of standards explicitly aiming for the de-consolidation of the internet. Internet consolidation refers to a process of increasing control over internet infrastructure and services[18] by a small set of organizations. The internet is known to be increasingly consolidated, or in other words, moving toward a larger fraction of traffic involving a smaller set of large content providers, social networks, and content delivery platforms.

In the IETF, and within other industry-driven internet SDOs, it is common to see large technological companies pushing for their own standards to become the norm for the rest of the internet.[19] There is a relative consensus[20] about the fact that only a few technological companies effectively have the capabilities to develop sophisticated technical proposals and push them in internet SDOs.

This situation is further amplified by the quasi-total control that large corporate actors leverage over certain parts of the internet, as a result of the growing consolidation of its many markets and infrastructure (such as DNS resolvers services as seen above).

Thus, supporting standards that directly contribute to the consolidation of the internet should not be on the European agenda. This does not mean that all standards promoted by large companies have to be considered negatively by default, especially given the current structure of the private internet governance regime,[21] which structurally empowers large technological companies to be responsible for most internet standards.

Even in this constrained realm, the focus of the EU should be to support standards that are aimed precisely at the de-consolidation of the internet. These efforts should be cognizant of the fact that "even when open protocols incorporate techniques intended to prevent consolidation, economic and social factors can drive users to prefer solutions built with or on top of supposedly decentralised technology."[22] Yet, and as indicated previously, the example provided by the EU Digital Markets Act is an inspiring example of how the crucial aspiration for

---

[18] Arkko, Jari. "The Influence of Internet Architecture on Centralised versus Distributed Internet Services." Journal of Cyber Policy 5, no. 1 (2 January 2020): 30–45.

[19] Harcourt, Alison, George Christou, and Seamus Simpson. Global Standard Setting in Internet Governance. Oxford University Press, 2020.

[20] Cath, Corinne. Eaten by the Internet. Meatspace Press, 2023.

[21] Haggart, Blayne, Natasha Tusikov, and Jan Aart Scholte, eds. Power and Authority in Internet Governance: Return of the State? 1st ed. Routledge, 2021.

[22] Nottingham, Mark. "Internet Consolidation: What Can Standards Efforts Do?" Internet Draft. Internet Engineering Task Force, 4 December 2022. https://datatracker.ietf.org/doc/draft-nottingham-avoiding-internet-centralization/06/.

interoperability[23] can be politically prescribed by public regulators and become addressed as a result by internet SDOs to address worrying patterns of consolidation.

B. MOVING AWAY FROM THE INTERCONNECTION NARRATIVE

While internet SDOs are formidable machines to create consensus on how to make the internet grow and "work better" (the official goal of the IETF), they appear much less equipped in relation to other types of societal or political norms. Discussions within and outside of the human rights protocol considerations (HRPC) research group of the Internet Research Task Force (IRTF) are a case in point of the relative resistance from many corporate engineers to see their work framed as political[24] and their opposition to the notion that specific political values can be enshrined in internet standards.

Yet, we know that internet standards can constitute substantive political issues[25] with direct implications for state actors, companies, or individuals alike. In this context, drawing on its human-centric inclination with respect to its digital policies, the EU should support the development and deployment of internet standards that are not solely focused on connecting more devices and making the network grow. This could be operationalized, for instance, through dedicated impact assessments. As convincingly argued by Paris et al.,[26] instead of being only fixated on the constant growth of global interconnection, standards should be oriented toward supporting more cooperativity between individuals and local communities, for example.

Internet standards have become in many ways "the default infrastructure for society."[27] Limiting latency or ensuring the security of communications are evidently positive objectives, and arguably in line with the interests of most internet users. Yet, the – rather understandable – fixation of internet SDOs on the efficiency and growth of the network prevents discussions on the actual implications of their deployment. The anthropologist Corinne Cath argues[28] in this sense that internet SDOs, such as the IETF, have engineered their own innocence in relation to the actual use and societal implications of the standards they formulate.

The EU approach should recognize this challenge by thinking more in terms of qualitative connectivity rather than plain quantitative interconnection, being more mindful of the magnitude of both positive and negative impacts generated by the internet's expansion across the world. As presented below, this shift would also require thinking of the internet not only as a

---

[23] Doctorow, Cory. The Internet Con: How to Seize the Means of Computation. Verso Books, 2023.

[24] Cath, Corinne. Changing Minds and Machines. Doctoral dissertation, University of Oxford, 2021.

[25] DeNardis, Laura. Protocol Politics: The Globalization of Internet Governance. MIT Press, 2009.

[26] Paris, Britt S., Corinne Cath, and Sarah Myers West. "Radical infrastructure: Building beyond the failures of past imaginaries for networked communication." New Media & Society (2023).

[27] Cath, Corinne. "Eaten by the Internet: Putting Internet Infrastructure Power on Your Radar." Tech Policy Press, 30 October 2023. https://techpolicy.press/eaten-by-the-internet-putting-internet-infrastructure-power-on-your-radar.

[28] Cath, Corinne. Changing Minds and Machines. Doctoral dissertation, University of Oxford, 2021.

critical infrastructure to be made bigger and more efficient but also recognize it as a space where individuals are increasingly subject to various forms of control and surveillance.

C. MORE ENCRYPTION, LESS NETWORK CONTROL

Standards supported by the EU need to empower individuals and end users who are confronted with the challenges of an increasingly digitized world. If internet SDOs, such as the IETF, have relatively failed to integrate societal norms and values into their agenda, they have been at the forefront of discussions on encryption and security. In the wake of the Snowden revelations a decade ago, internet SDOs have developed sophisticated ways to encrypt and protect communications – which have become standard practices across the world and which the European Commission has also supported over recent years by promoting IETF's DNSSEC specifications to secure DNS data, for instance.

Yet, in the meantime, EU Member States and specific Directorates-General (DGs) of the European Commission (including the DG for Migration and Home Affairs) have promoted a policy agenda that appears adversarial to the deployment of encryption techniques over the internet, while favoring more network control. This fight against encryption is front and center in the current EU negotiations on the CSAM regulation, for example. Instead of weakening encryption, requesting backdoors, or considering the use of secure messaging tools (such as Signal) as a self-incriminating act (see in France), the EU should vocally support people-centered privacy-protecting protocols.

This indirectly relates to discussions occurring in more formal and state-centered internet SDOs, such as the Technical committee of the International Telecommunication Union (ITU-T). New technical proposals led by China[29] (labeled as "New IP") underline the ambition of a number of countries to reshape fundamental protocols on which the internet relies to get more visibility and control over the networks. Countering these developments has been presented by the EU as an important political priority. The European Commission has invested significant political capital at the international level to leverage influence over these technical processes and prevent proposals that favor more state-based network control from becoming a reality. This report highlights that the direction of the EU's internal policies in relation to encryption weakens its simultaneous claims grounded in human rights against state-centered network control in the context of internet SDOs such as the ITU.

This section thus argues that adding these three new dimensions – de-consolidation of the internet, push for greater cooperativity, and support of individuals' privacy and autonomy – would bring added value and greater coherence to the EU agenda in relation to internet standards.

[29] Nanni, Riccardo. "Digital sovereignty and Internet standards: normative implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force." Information, Communication & Society 25, no. 16 (2022): 2342-2362.

But what also matters is how these standards are adopted and the "openness" of these processes for different types of stakeholders – and, most importantly, civil society – in contributing to their formulation.

Supporting more openness in internet standardization processes

In the field of internet standardization, the current status quo – namely the predominant private industry-driven regime – falls short in terms of democratic accountability, legitimacy, and inclusion.

As evidenced by the 2022 standardization strategy and the role given to ESOs in the context of new EU digital policies, participation and representativeness in technological standardization processes are an important area of priority for the European Commission. However, as for other domains, the EU's approach appears characterized by several inconsistencies resulting from competing political, security, and economic objectives presented above. The new European Commission approach toward internet standards should support the opening of new ways to effectively contribute to the making of internet standards for actors that are not large technological corporations. These efforts should aim at de-privatizing standard-setting, broadening participation, and politicizing standards.

A. DE-PRIVATIZING STANDARD-SETTING

The literature on the feudalization of the internet[30] describes at length the power and control accumulated by large technological companies over the internet, which evolved, according to Tim Wu,[31] from "a freely accessible channel to one strictly controlled by a single corporation or cartel – from open to closed system."

The approach of the EU in relation to technology standardization has been grounded for decades, if not longer, in the belief that industries are better suited to lead such processes. Micklitz makes the argument[32] that "the relocation of knowledge from the administration to industry is the result of a process that dates back to the late 19th century and begins with industrialization," underlining the emergence of vast discrepancies in the technical expertise held within state bureaucracies and large technological companies.[33]

In relation to the internet, the current legitimacy of this largely private-driven standardization process falls short. The words of Ben Tarnoff[34] and his critique of the industry-dominated internet are essential in this context: "Understanding how privatization made the modern internet is essential for any movement that seeks to remake it. Movements must know their

---

[30] Tréguer, Félix. L'utopie Déchue. Fayard, 2019.

[31] Wu, Tim. The Master Switch: The Rise and Fall of Information Empires. Vintage, 2011.

[32] Micklitz, Hans-W. The Role of Standards in Future EU Digital Policy Legislation. Report of ANEC and BEUC, 2023.

[33] A similar argument is made by Mariana Mazzucato in The Entrepreneurial State.

[34] Tarnoff, Ben. Internet for the People: The Fight for Our Digital Future. Verso Books, 2022.

enemy. If they expend their energy on the wrong target, the opportunity for meaningful change is lost. History shows why privatization is the right target, how it forms the common foundation for the diverse dysfunctions and depredations of the modern internet."

Though a strictly multilateral governance regime for internet standards is evidently not a desirable option from a human rights standpoint, the EU should support the emergence of an internet standardization regime that is not captured – or even saturated – by a few multinational corporations. This effort could take the form of enhanced political exchanges with internet SDOs to discuss how their policies related to inclusion and transparency could be improved, based on the practices and guidelines developed by the EU through its European standardization system, for instance. These exchanges could be nurtured through bilateral activities, similar to those of the Internet Society, aimed at familiarizing policymakers with the work of the IETF, and vice-versa.

This recommendation does not suggest, however, that the general practices of ESOs in relation to participation and transparency are to be systematically followed by internet SDOs. The openness of the standardization processes of both ETSI and CEN-CENELEC is notoriously problematic. Neither the minutes of working group meetings nor their actual composition are made public. The standards themselves are often protected by intellectual property rights and are not made available free of charge. Admittedly, this is in stark contrast with the practices of other SDOs such as the IETF or W3C. Nonetheless, EU policies in relation to the inclusion of non-commercial stakeholders, granting them special rights and formal membership in the standard development process, could be an interesting avenue to consider for such SDOs.

B. BROADENING PARTICIPATION

While there are merits to reaffirming the EU's agency in standard-setting, the EU discourse often fails to recognize and address the unintended consequences of its own initiatives, such as accelerating the growing "trend in state-based rule-setting on Internet infrastructure."[35] Instead of normalizing the power of digital monopolies or state-based approaches to internet infrastructure, the EU should support civil society and citizen engagement and their effective participation in internet standardization processes.

While the project StandICT is a first step in the direction of supporting more European voices (with presumably limited means) to attend these standardization arenas, the limited scale of this project, which funds a hundred experts for the whole ICT standardization field, underscores the limits of the current EU approach. Mirroring the comments made by Micklitz[36] in 2023 in reference to EU technical standardization policy, current initiatives designed to secure the meaningful participation of all concerned stakeholders in internet SDOs looks more "like a fig leaf" than a structural policy.

---

[35] ten Oever, Niels. Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure. Doctoral dissertation, University of Amsterdam, 2020.

[36] Micklitz, Hans-W. The Role of Standards in Future EU Digital Policy Legislation. Report of ANEC and BEUC, 2023.

For instance, the input of European civil organizations within IETF is infinitesimal, and greater funding should be allocated in order to foster the effective participation of civil society and citizens in this area.

Also, the EU should not remain strictly focused on the European scale when it comes to participation and funding support. The EU would benefit from broadening participation in standardization processes to actors that are usually not included in these technical arenas, regardless of their location, as long as they promote an internet centered around people and the public interest.

C. POLITICIZING STANDARDS

Internet SDOs, such as the IETF, are not used to answer the normative, political, or societal issues that their standards may generate – a pattern that also characterizes technological standardization as a whole. Internet SDOs, like international organisations,[37] often depoliticize their work as a way to keep themselves out of politics. This is reflected in their organizational cultures and the professional habits of their individual members. This has positive implications – for instance, in terms of efficiency and trust – that fall short in comparison to the negative aspects, including the dire lack of accountability of these processes.

The EU should support the politicization of these technical discussions. Politicizing does not mean making them subject to the direct control of political governments or state actors. On the contrary, it means formulating them in the open and raising the public awareness of the political implications of those technical deliberations, allowing individuals and social groups to be aware and discuss their implications, and support relevant communities to participate in these arenas. Participation from all the various concerned publics seems essential before such standards become effectively enacted and gradually shape the invisible infrastructure of the internet.

The work of Jean-Christophe Graz and Christophe Hauert has shown how the "importance of socio-technological choices enacted in standards gives civil society organizations a strong incentive to be involved" in standard-setting. Despite obvious resource asymmetries, it is common practice to see "reputation-sensitive firms" accommodating (at the margins) some civil society demands in standardization processes, partly as a way to legitimize those processes and give them greater credibility. These successes could fuel more participation from non-commercial actors.

Yet, despite these obvious benefits, civil society participation does not have to be imposed at any cost. Indeed, the risk run by civil society actors to become instrumentalized in industry-driven standardization processes is real. The participation of civil society actors needs to be supported in contexts where their contribution will be valued and recognized, and where their positive contribution may trump their indirect support and legitimation of such private governance arrangements.

---

[37] Louis, Marieke, and Lucile Maertens. Why International Organizations Hate Politics: Depoliticizing the World. Routledge, Taylor & Francis Group, 2021.

The fact that almost no European civil society organizations can be found in the list of IETF participants over recent years is a testimony of the necessary steps to be taken to inform public interest stakeholders that would clearly benefit from being exposed to these technical conversations. The EU could improve its policies by communicating (in different languages) about the political issues currently at stake in internet SDOs, or directly support projects that contribute to the simplification of technical discussions, as exemplified by Article 19's new Internet Standards Almanac. But awareness is evidently not the only obstacle preventing the participation of such groups. The lack of technical expertise – and the often-missing involvement of public interest technologists – within civil society organizations is a major challenge in Europe and beyond. In the context of a shrinking space for civil society and worries about the lack of funding currently available for digital rights organizations, the EU should address this challenge through more direct funding and capacity-building activities directed toward civil society.

These six high-level policy recommendations show that the EU would greatly benefit from a renewed policy approach toward internet standards, with the aim of strengthening the internet's openness, as further elaborated in the concluding section.

CONCLUSION: BUILDING AN ALTERNATIVE IMAGINARY AND TRAJECTORY FOR THE FUTURE OF THE OPEN INTERNET

> *"Making it possible for the world's computers to talk to one another was an impressive technical achievement. Making this machinic conversation serve an end other than infinite accumulation will be a political one. It may seem unlikely, but so was the internet. History is filled with improbable turns that look inevitable in retrospect. The future will be too." - (Tarnoff, 2022)*

The internet is contingent. It is the result of technological and political choices and imaginaries that, over the course of half a century, gradually shaped its unique structure and the affordances it grants to its multitude of users – be they states, companies, or individuals.

The current status quo for internet standard-setting, namely the predominant private industry-driven regime, falls short in terms of democratic accountability, legitimacy, and inclusion. This model also does not appear well-equipped to address worrying patterns of market consolidation and power shifts favoring a few large technological companies.

Over recent years, the EU has entered this policy field in various ways, and at times precisely to address these well-identified challenges. In doing so, this report underlines that the EU has recently attempted to assert itself into the internet architecture, with both positive and negative implications, while pushing its agenda for EU digital sovereignty. These attempts have created inconsistencies, and even incompatibilities, between the EU's policy objectives of asserting more control through and over the internet, and its overarching goal to protect it as a global and open network.

These inconsistencies highlight the fact that the EU is still torn between different objectives – which limits the consistency and success of its policies. While a global supporter of multistakeholder internet governance, the EU is pushing toward a form of regionalization of standard-setting through the 2022 EU standardization strategy. While promoting the deployment of state-of-the-art encryption protocols, the Commission proposes to weaken the use of encryption through the recent CSAM legislative proposal. While flexing its regulatory muscles to curb the power of Big Tech, it does not structurally challenge its predominance in internet standard-setting but rather normalizes the outcomes of existing industry-driven processes.

In 2024, the next European Commission's mandate will give an important opportunity for the EU to frame a new vision for what could become the future of the European Open Internet agenda. This report provides recommendations that are expected to pave the way for an alternative path for EU digital policies, conducive to more openness for the future of the internet. The Table below summarizes what should be the main avenues of this new approach. It contributes to the emerging body of work, supported in part by the Open Future Foundation, aiming at re-imagining the internet and building infrastructures for the public good.

I. SUPPORTING STANDARDS FOSTERING MORE INTERNET OPENNESS	
De-consolidating the internet	Support the deployment of standards explicitly aiming to address internet consolidation, and prescribe interoperability when relevant.
Moving away from the interconnection narrative	Support "meaningful connectivity" rather than plain quantitative interconnection to foster cooperativity through the networks.
More encryption, less network control	Support people-centered privacy-protecting protocols instead of promoting an adversarial policy approach to the deployment of encryption techniques.
II. SUPPORTING MORE OPENNESS IN INTERNET STANDARDIZATION PROCESSES	
De-privatizing standard-setting	Create exchanges with private internet SDOs to discuss how inclusion and transparency could be improved – for instance, based on the practices and guidelines developed by the EU.
Broadening participation	Allocate greater funding to foster the effective participation of civil society and citizens in this area, both at European and global levels.
Politicizing standards	Improve EU policies to communicate around the political issues in internet SDOs, and support projects that contribute to raising the awareness around these technical discussions.

BIBLIOGRAPHY

Abbate, Janet. *Inventing the Internet*. MIT Press, 2000.

Andersdotter, Amelia, and Lukasz Olejnik. "Policy strategies for value-based technology standards." *Internet Policy Review* 10, no. 3 (2021): 1-26.

Barrinha, André, and George Christou. "Speaking sovereignty: the EU in the cyber domain." *European Security* 31, no. 3 (2022): 356-376.

Bartley, Tim. "Power and the Practice of Transnational Private Regulation." *New Political Economy* 27, no. 2 (2022): 188-202.

Bellanova, Rocco, Helena Carrapico, and Denis Duez. "Digital/sovereignty and European security integration: an introduction." *European Security* 31, no. 3 (2022): 337-355.

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020.

Broeders, Dennis. T*he public core of the Internet: An international agenda for Internet governance*. Amsterdam University Press, 2016.

Broeders, Dennis, Fabio Cristiano, and Monica Kaminska. "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions." *JCMS: Journal of Common Market Studies* 61, no. 5 (2023): 1261-80.

Cath, Corinne. *Changing Minds and Machines.* Doctoral dissertation, University of Oxford, 2021.

Cath, Corinne. *Eaten by the Internet*. Meatspace Press, 2023.

Christou, George, and Seamus Simpson. "Gaining a stake in global internet governance: the EU, ICANN and strategic norm manipulation." *European Journal of Communication* 22, no. 2 (2007): 147-164.

Claessen, Eva. "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, no. 1 (2020): 140-157.

Couture, Stephane, and Sophie Toupin. "What does the notion of 'sovereignty' mean when referring to the digital?" *New Media & Society* 21, no. 10 (2019): 2305-2322.

Daucé, Françoise, and Francesca Musiani. "Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction." *First Monday* 26, no. 5 (2021).

Doctorow, Cory. *The Internet Con: How to Seize the Means of Computation*. Verso Books, 2023.

Graz, Jean-Christophe & Christophe Hauert. “Translating Technical Diplomacy: The Participation of Civil Society Organisations in International Standardisation.” *Global Society* 33, no. 2 (2019): 163-183.

Harcourt, Alison, George Christou, and Seamus Simpson. *Global Standard Setting in Internet Governance*. Oxford University Press, 2020.

Hoffmann, Stacie, Dominique Lazanski, and Emily Taylor. "Standardising the splinternet: how China's technical standards could fragment the internet." *Journal of Cyber Policy* 5, no. 2 (2020): 239-264.

Karjalainen, Tyyne. "European Norms Trap? EU Connectivity Policies and the Case of the Global Gateway." *East Asia* (2023): 1-24.

Mager, Astrid. “European Search? How to counter-imagine and counteract hegemonic search with European search engine projects.” *Big Data & Society* 10, no. 1 (2023).

Micklitz, Hans-W. *The Role of Standards in Future EU Digital Policy Legislation*. Report of ANEC and BEUC, 2023. URL: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf

Musiani, Francesca. "Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices." *Information, Communication & Society* 25, no. 6 (2022): 785-800.

Nanni, Riccardo. "Digital sovereignty and Internet standards: normative implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force." *Information, Communication & Society* 25, no. 16 (2022): 2342-2362.

Paris, Britt S., Corinne Cath, and Sarah Myers West. "Radical infrastructure: Building beyond the failures of past imaginaries for networked communication." *New Media & Society* (2023).

Perarnaud, Clément, and Julien Rossi. "The EU and Internet standards–Beyond the spin, a strategic turn?" *Journal of European Public Policy* (2023): 1-25.

Perarnaud, Clément, Julien Rossi, Francesca Musiani, and Lucien Castex. "'Splinternets': Addressing the renewed debate on internet fragmentation." Parlement Européen; Panel for the Future of Science and Technology (STOA), 2022. DOI: https://data.europa.eu/doi/10.2861/183513

Russell, Andrew L. *Open Standards and the Digital Age*. Cambridge University Press, 2014.

Seidl, Timo, and Luuk Schmitz. "Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy." *Journal of European Public Policy* (2023): 1-28.

Tarnoff, Ben. *Internet for the People: The Fight for Our Digital Future*. Verso Books, 2022.

ten Oever, Niels. Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure. Doctoral dissertation, University of Amsterdam, 2020.

ten Oever, Niels. "Norm conflict in the governance of transnational and distributed infrastructures: the case of Internet routing." *Globalizations* 20, no. 1 (2023): 184-200.

Tréguer, Félix. *L'utopie déchue*. Fayard, 2019.

Wu, Tim. *The Master Switch: The Rise and Fall of Information Empires*. Vintage, 2011.

ABOUT OPEN FUTURE

Open Future is a European think tank that develops new approaches to an open internet that maximize societal benefits of shared data, knowledge and culture.

Clément Perarnaud is a Postdoctoral Researcher at the Brussels School of Governance (BSOG-VUB). He holds a Ph.D. in political science from the University Pompeu Fabra (UPF, Barcelona). In 2023, Perarnaud was a fellow at the Open Future..

ACKNOWLEDGMENTS

I would like to thank Zuzanna Warso, Alicja Peszkowska, Paul Keller, and Alek Tarkowski for their excellent feedback and support throughout the fellowship. I am also grateful to Julien Rossi for his always insightful thoughts on the EU's standardization approach, and to the anonymous experts who shared their time and comments on earlier drafts.