



**Shifting terrain:
“Standards, Protocols, Ecosystem”
Report on a round-table discussion**

**Maxigas & Alek
Tarkowski**

**critical
Infrastructure
lab**

The logo icon for Critical Infrastructure Lab, consisting of a stylized, jagged line forming a shape reminiscent of a mountain range or a circuit board trace.

Shifting terrain: “Standards, Protocols, Ecosystem”

Published by the critical infrastructure lab,
Amsterdam, October 2023.

Shifting terrain: “Standards, Protocols, Ecosystem” –
Report on a round-table discussion © 2023 by Maxigas &
Alek Tarkowski is licensed under Attribution-
NonCommercial-ShareAlike 4.0 International.
<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Set in Source Sans, Source Serif and Source Code fonts.

Made with free software from plain text:
<https://doi.org/10.5281/zenodo.8412230>
DOI 10.5281/zenodo.8412230

critical infrastructure lab document series
CIL#006

DOI FIXME

Open Future
<https://openfuture.eu/>

critical infrastructure lab
<https://www.criticalinfralab.net/>

Table of Contents

Workshop participants	2
Introduction	3
Protocols and power	5
Identity	8
Interoperability	16
Standards	19
Action points	22
References	23

Acknowledgements

This work was generously supported by the Ford Founcation [grant number 144895, 2022] and the Digital Impact and Governance Initiative (DIGI) at New America.



Workshop participants

Open Future and the critical infrastructure lab co-organised a round-table discussion on “*Standards, Protocols, Ecosystem*”. The discussion took place in Amsterdam and online on the 20th of June, 2023. This report is an attempt to share lessons learned in the spirit of “learning in the open”.

The following people contributed to the round-table discussion. We are particularly grateful to people providing introductory remarks for the specific sessions: Ian Brown, Mallory Knodel, Amandine Le Pape, and Michael Veale.

- ◆ Alberto Cerda Silva (Ford Foundation)
- ◆ Allison Price (New America Foundation)
- ◆ Amandine Le Pape (Matrix)
- ◆ Andreas Baur (Amsterdam Institute for Social Science Research, International Centre for Ethics in the Sciences and Humanities)
- ◆ Bertrand De La Chapelle (The Datasphere Initiatives)
- ◆ Clement Perarnaud (Centre for European Policy Studies)
- ◆ Corinne Cath (critical infrastructure lab)
- ◆ Dietrich Ayala (Protocol Labs)
- ◆ Ian Brown (Fundação Getulio Vargas)
- ◆ Jan Penfrat (European Digital Rights)
- ◆ Jordan Usdan (Microsoft)
- ◆ Julian Ringhof (European Council on Foreign Relations)
- ◆ Liv Kittel (Spitfire Strategies)
- ◆ Maarit Palovirta
(European Telecommunications Network Operators’ Association)
- ◆ Mallory Knodel (Center for Democracy and Technology)
- ◆ Mathilde Sanders (University of Utrecht / PubHubs)
- ◆ Michael Brennan (Ford Foundation)
- ◆ Michael Veale (University College London)
- ◆ Niels ten Oever (critical infrastructure lab)
- ◆ Pamela Gil-Salas (Umeå University)
- ◆ Paul Keller (Open Future)
- ◆ Robin Berjon (Protocol Labs)
- ◆ Ross Creelman
(European Telecommunications Network Operators’ Association)
- ◆ Sivan Pätsch (Open Forum Europe)
- ◆ Surana Aditi (University of Edinburgh)

Introduction

**a policy program that can
serve as a long-term
reference point**

Today's world-wide web is powered by the original open web protocols, overlaid with proprietary platforms that often place private interests over public interest. This has an adverse impact on trust, competition, and democratic values. Ford Foundation, New America's Digital Impact and Governance Initiative, and Microsoft – the leading organisations in the Missing Layers collaborative – have described this condition as the case of missing layers of a digital ecosystem that is people-centric, functions as a digital commons, and is enabled by open protocols.

The Missing Layers collaborative aims to “develop an actionable vision for digital technology to counter present harms and chart a path towards a jointly designed and shared digital infrastructure that can enable a democratic technology ecosystem.” The group has identified four areas where this vision of open protocols combined with public interest governance could be applied: data sharing, communication, identity control, and payments.

The collaborative focuses on governance, understood as a combination of government regulation, participatory processes, and competitive innovation in digital ecosystems. One of the goals of this collaborative is also to seek designs that build on the principle of openness to balance innovation with the protection of fundamental values.

The round-table on “Protocols, standards, ecosystems” was organised by Open Future and the critical infrastructure lab as part of the process to develop the Missing Layers framework. We were interested in contributing to the Missing Layers conversation with a perspective of European public interest advocates. We wanted to take into account the specificity of the European context, where digital ecosystems are increasingly subject to government regulation, aimed at securing some of these public interest goals.

Our aim was to explore how the principles of sovereignty and interoperability can be secured through protocol governance and how the two principles interact. What kind of sovereign powers and forms of interoperability do we need? And how does protocol and standards governance interplay with legislative measures?

Through this conversation, we also aimed to identify areas where the vision of a democratic technology ecosystem can be brought to life. We want to identify principles and elements of a

policy program that can serve as a long-term reference point for public interest advocacy and European policymakers. ○

Protocols and power

infrastructural ideologies as a strategically deployed set of narratives and metaphors

Infrastructural ideologies and network paradigms

The critical infrastructure lab published a draft report to discuss at the event,⁰¹ introducing a framework to study protocols, standards and governance. The framework defines three network paradigms that describe how power is exercised differently through differently engineered and governed networks. The three network paradigms are the Internet (“open internetworking”), GSM (“cellular mobility”) and 5G (“smart networks”).

Potential users of these networks need to be enrolled as *actual* users of the networks. The framework defines infrastructural ideologies as a strategically deployed set of narratives and metaphors,⁰² engineering principles and material constraints,⁰³ as well as governance structures⁰⁴ and political-economic incentives. All these very different constituents of infrastructural ideologies are deployed in order to legitimise the network as a rational solution and justify users’ reliance on it. In order to do so, infrastructural ideologies highlight some aspects of the network functions in order to leave other aspects out of the limelight. The infrastructural ideology gives users good reason to be users, that is to say to subject themselves to the regime of power encoded in the infrastructure by occupying the subject positions that it defines. A successful infrastructural ideology leads to wide adoption and popularity with users, while at the same time serving the vested interests of its instigators.

01 <https://www.criticalinfralab.net/uploads/2023/07/missingreport.pdf>↵

02 More precisely referred to as “sociotechnical imaginaries” in Science and Technology Studies.↵

03 The so-called “infrastructural effects”.↵

04 For example, the standards bodies and their standardisation processes.↵

Sovereignty and interoperability

Sovereignty is traditionally defined as the ultimate authority over a territory circumscribed by borders and the subjects that are attached to that territory.⁵ On the one hand, there is a long-standing link between the concept of sovereignty and the military control of a land. On the other hand, sovereignty is exercised over subjects, who are subjects to the sovereign power. All in all, sovereignty today usually refers to the relationship between the modern state, its territory, and its citizenship.

Modern political and legal theory uses the concept of sovereignty to explain why states can define laws, and to be in some sense above the law themselves. While sovereignty is the manifestation of human freedom on Earth, it is also what allows states to control their citizens. Sovereignty is the basis of international relations where nation states face each other nominally as equal (ultimate) powers:

Sovereignty is a hypothetical trade, in which two potentially (or really) conflicting sides, respecting de facto realities of power, exchange such recognitions as their least costly strategy. (Wallerstein 1991, 44)

Standards and protocols organise space and time to produce subject positions. Users of the protocol occupy these subject positions, either intentionally or unintentionally. When they do so, they fall under the regime of power defined by the operation of a protocols stack. Protocols for authentication have the infrastructural effect to bring transform the user into a subject of a sovereign entity. From this vantage point, interoperability becomes a question of power.

Interoperability is the property of technologies to work together, so that we can plug any electric appliance into an electric wall socket and the plug would fit. The question of interoperability is even more crucial for communication protocols that connect to systems, in this case any one system is as useful as it is interoperable with another system. Standards are responsible for ensuring interoperability in technologies and protocols are specific to communication.

Interoperability is thus a way to extend the reach and scope of a protocol stack throughout the infrastructure, enrolling users into its regime of power, but also to negotiate the entanglements of power between different sovereignties. Even though interoperability allows interconnection in communication protocols, the real question is on whose terms does interconnection happens. At different points in history, the United States, and European nation states were in this position to define the terms of interconnection, when they introduced the network paradigm of open

**interoperability is the
property of technologies to
work together**

internetworking and cellular mobility. At this historical moment, the burning question of the day is whether China's bid to do the same with the 5G protocols stack could work, and with what consequences.

○

05 Following German political theorist Carl Schmitt, a prominent member of the Nazi party.↵

Identity

Case studies of identity protocols

Two case studies were presented at the round-table, applying the proposed framework to contrast two authentication protocols: OpenID and Aadhaar. These protocols represent very different approaches to digital identity, from their problem definitions to their threat models. What we learn from comparing them is that a digital identity protocol is as useful and powerful as the sovereignty that is backing it up.

OpenID: is a weak identity protocol by design, targeting a global market of digital services. It allows a user to log in to a web service using credentials registered at with another web service. Thus, users can choose their identity providers based on trust and convenience, and use that identity to access interoperable services without registering with them separately.

The large OpenID players in terms of the standardisation process and the adoption of the protocols are drawn from the ranks of US Silicon Valley capital, including the famous digital platform monopolies (GAFAM – Google, Amazon, Facebook, Microsoft). Philosopher of technology Benjamin Bratton (2015) claims that these companies acquired some aspects of sovereignty that are comparable to nation states. Bratton's provocative idea was that corporations, not just nation states, can be sovereign. The idea gained traction in the last few years, when governments subjected these companies to increased scrutiny and regulation in the EU, the US, and elsewhere.⁶

a digital identity protocol is as useful and powerful as the sovereignty that is backing it up

Rather than any perceived issue with content moderation, democratic oversight, procedural transparency, market competition, user data, surveillance practices and privacy policies, what really changed to open the possibility of regulation might have been that nation states actually recognised these companies as one of their own: as fledgling sovereign entities operating within their territory. According to this interpretation, states started regulating platforms because they saw them as challengers to their exclusive powers, e.g. their sovereignty.

The ideological catch of OpenID is similar to the promise of the open web. While any capable actor can participate in the market of identity provision, only big players are in the position to take

advantage of being identity providers. Small players can choose whether to participate as interoperable parties that accept OpenID logins, which effectively enrolls them as well as their users in the regime of identity established by US capital. As a result, OpenID adoption steadily fell, reverting back to an ecosystem where its place has been taken over by APIs provided by the same monopolies.

Aadhaar: is a strong identity protocol by design, targeting people in India. It is backed up by the state and only used within its territory, so that the sovereignty in question here is the traditional sovereignty of a nation state. This is in obvious contrast with OpenID, which targets a global market of web services with platform providers as the sole actors.

Aadhaar is tied to materiality and the land in various ways. As a proof of residence, it established its subject as dwelling in the geographical territory of India, and subject to its laws. Citizens' biometric data such as retina scans and fingerprints tie this technical and legal identity to the properties of their physical bodies. The identity is issued as a physical card in addition to database entries and API access. SIM cards can be connected to the Aadhaar identity as additional networked physical tokens identifying the user.

Being a strong identity protocol means that Aadhaar can be used for a variety of purposes beyond authenticating with web services. As critiques have pointed out, the identity protocol acts as a gatekeeper for access to state subsidies, health care, bank loans and everyday purchases, ultimately allowing or constraining the exercise of civil and consumer rights. The power of the protocol to establish interoperability between public and private service provision have itself been the target of controversies.

These examples warrant observations about the interaction of sovereignty and identity. Such reflections are especially pertinent in light of the initiative to establish a European digital identity (eIDAS). In particular, the European idea is to separate a “trusted and secure e-ID”⁷ from a future “digital euro” as a “complement to cash”.⁸ The approach is designed to avoid both the weak identity of OpenID that only works with web services and the over-powerful identity of

Aadhaar that crosses the line between commercial markets and public services.

06 Notably, they have been tightly regulated in China since their entry to that market, which has been precisely the reason for their exit from that market, creating the opportunity for national champions to take their place.↵

07 <https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation>↵

08 https://finance.ec.europa.eu/digital-finance/digital-euro_en↵

**civil society actors should
follow the process of eIDAS
and the Digital Euro**

Still, interoperability will be a key concern given the limited administrative integration and extensive sovereign powers of European nation states. As with other recent innovative European digital policies such as Gaia-X and the AI Act, certification for compliance and interoperability will play a major role. Digital rights advocates and civil society actors should follow the process of eIDAS and the digital euro closely and take clues from the experience of previous identity protocols in interventions to safeguard the public interest.

Structure and agency in standards bodies

The framework shows a neat picture of sovereign actors projecting their power through the development, implementation and deployment of standards and protocols, even whole network paradigms, which are adopted by users who subject themselves to the power of these sovereigns because they are convinced by their infrastructural ideologies.

The real process is much more complex, laden with historical contingencies, path dependencies, and the haphazard agency of engineers as deeply situated actors with quite some distance from the sovereign powers these standards and protocols are supposed to serve. It would be too simple to assume that participants in standards bodies are fully conscious of the larger interests they serve, or even that they can fully predict the consequences of their technical choices. These twists and turns have been extensively documented by historians of technology (Abbate 1999; Hillebrand 2001; Russell 2014).

**The power of ideology is to
define common sense**

On the Internet side, participants of the process saw protocol design mainly as struggle against material agency, e.g. getting things to work. The mandate and funding for the initiative has been provided by government funding through the Defence Advanced Research Projects Agency (DARPA), soon renamed simply to Advanced Research Projects Agency (ARPA), reflecting a US doctrine of demilitarising innovation at the end of the Cold War. Such atmosphere provided much intellectual freedom to participants, who disposed rather freely of their ample funding and made liberal use of the strong research environment. A case in point is that many Requests for Comments (RFC) that defined the actual protocols have been written and/or implemented by graduate students. It is entirely plausible that they were largely unaware of, or unconcerned about the geopolitical power struggles in which establishing a new network paradigm would strengthen US hegemony and secure access to a global market.

Attributing an infrastructural ideology to the network paradigm of the Internet may sound like its designers carried out a pre-formulated plan to dupe the world. However, ideology does not work through individual consciousness, intentionality or agency.

Most engineers who worked on the development, implementation and deployment of early Internet protocols were as much under the influence of its infrastructural ideology as their users in the subsequent decades. The power of ideology is to define common sense, rationality and the public interest in a way that the ensuing consequences serve partial interests.⁹ That the individual historical actors in standards bodies are experiencing their contributions and their difficulties as spontaneous, contingent and practical, is nothing else but the very proof of the successful performance of an ideology.

The idea of the market is a case in point. The market plays an important role in US common sense about the public interest, such as in providing consumers a free choice for exercising their purchasing powers, and innovators a medium to offer products and services to those consumers. In such a capacity, the market is a key component in the ideology of the American Dream, a trope familiar to citizens and would-be citizens of the country.¹⁰ While this is not a very original argument, it may account for the reason why US engineers working on the early Internet may find it common sense to design protocols that distribute power in the manner of markets.

09 Corinne Cath, a participant in the round-table and fellow of the critical infrastructure laboratory, diagnoses the same point about the ideology of patriarchy at work in standards bodies (2023). In her case study of the Internet Engineering Task Force (IETF) — the epitome of open process — it is clear that it is not attendees' evil intentions, or preconceived plans, that prevent womens' participation in standardisation on equal grounds to men. On the contrary, it is exactly that participants spontaneously follow what they take as a common sense approach to valuation and behaviour in the IETF, whose consequences are nonetheless detrimental to women's contributions.↵

10 And due to the cultural imperialist strategy of the US, to an increasingly global audience as well.↵

US capital was in a position to take advantage of the global reach of the online open market

But what happens after an ideology is inscribed in a protocol stack, and that protocol stack is canonised as a global network paradigm? Like the question of individual agency, the cause-effect relationship between protocol design and the projection of political power across borders is an elusive one. There are good reasons to believe that open protocols and the open process of standardisation served US interests, market expansion, geopolitical ambitions in the 1990s. On the one hand, the US government held reigns in the world of Internet Governance, with the US Chamber of Commerce owning the root zone file in which every top level domain is recorded.¹¹ On the other hand, US capital was in a position to take advantage of the global reach of the online open market and the permissionless innovation enabled by the End-to-End principle enshrined in TCP/IP. These material conditions cemented US hegemony to some degree, but also created ideological contradictions and path dependencies.

Ideological contradictions meant that the US came under fierce criticism from its partners and enemies for advertising the doctrine of openness and collaboration in the development and governance of the Internet, while keeping control of the most obvious choke point within its underlying infrastructure. The US gave up its hold on the DNS root zone file on the 1st October, 2016. Around the same time, East Asian multinational corporations began to appear as viable competitors to US platform monopolies in the lucrative market of online services.¹² The infrastructural ideology of open internetworking and the protocol design of the TCP/IP stack meant that US state and capital could do little to halt their advance. Both US incepted material conditions and governance institutions now played to the advantage of foreign actors. Once the terms of interconnection have been set in the context of a network paradigm, the US could do as much to turn them around as Victor Frankenstein to control the Creature.

11 The last part of web addresses such as .net or .nl.↵

12 Prominent examples are the Alibaba online marketplace, Sina Weibo social media platform and the super-app WeChat.↵

Structure and agency in user adoption

In this round-table discussion, we look at power and agency from the point of view of standards and protocols, interoperability and sovereignty. An assumption that comes with the topic is that the grammars defined by standards and protocols for interoperable machine-to-machine communication are as much instruments of power than the software interfaces running on the application layer and the content delivered by the network to end users. By focusing on low-level technological solutions and their governance mechanisms, we are privileging a bottom-up view of the protocol stack and the social relations it enables and instigates.

Overemphasising the role of the underlying *infrastructures* and its infrastructural effects such as interoperability may lead to losing sight of the real driver behind changes in the ecosystem of protocols and standards: user adoption. Our discussion is far removed from the perspective of end users who encounter infrastructural assemblages in the situated context of their life-worlds, while they focus their attention on getting mundane things done. When they do, their technological choices are rarely motivated by an evaluation of governance mechanisms or even technical suitability. Availability, reliability and convenience drive user adoption.

The example of Apple's experience design is a case in point. The free software movement has long been evangelising the adoption of user controlled technologies for political, aesthetic and practical reasons. In doing so, the free software movement often stood in for the public interest, articulating how technology in the service of users should work. While hackers have been waiting for the Year of the Linux Desktop¹³ that never comes, Apple championed a vision of technology that is simple and functional.

The point is that for most end users, the accessibility that Apple marketed proved to be more substantial than the promises of the free software movement. Apple focused its offering on the surface layer of the stack because that is where end users make their choices. The free software movement lost out because it has put the bulk of its efforts into improving the underlying infrastructure-level technologies rather than the associated user interfaces.

the accessibility that Apple marketed proved to be more substantial than the promises of the free software movement

The moral of the story is that the popularity, and, by extension, the power of protocols largely depends on which user interfaces and user-facing services choose to integrate them. ○¹⁴

13 Ironically, a subcultural reference to the historical tipping point marking the mass adoption of the GNU/Linux operating system by end users on their personal computers.↵

14 Cf. the discussion on user agents at the end of the “Challenges to open standard setting” section.↵

Interoperability

Interoperability is a principle that get constantly repeated in discussions about a more democratic internet. One that secures the goals of market competition, but which also brings with it greater innovation in services, and a chance for more society-centric solutions. In Europe, a range of interoperability mandates was or is in the process of being introduced - making it possible to discuss how state regulation enables the creation of interoperable ecosystems.

Interoperability mandates are an enabling force

There are signs that online ecosystems are shifting back to decentralised solutions, after a period of centralisation around the major platforms. And while interoperability is often mentioned as an important principle, it is hard to imagine Big Tech to create interoperable solutions on their own. The case of messaging interoperability rules and the Matrix protocol show how regulation can enable market change, if coupled with sufficient capacity to implement alternative, interoperable solutions.

**state regulation that is the
real enabler of interoperable
messaging**

Matrix is an open standard for secure, decentralised communication that aims to create an open communication layer on the web, to break communication silos. The messaging networks built on this protocol have 100 million individual users - many of them through governments or enterprises that adopted the standard. Matrix has been created in 2014, and observed significant growth whenever dominant communication networks have been failing to meet user expectations - such as when changes were made to WhatsApp's privacy policies.

Yet it is state regulation that is the real enabler of interoperable messaging. Matrix is expected to further grow when the Digital Market Act's interoperability requirements go into force, at the start of 2024. The act requires large online platforms and corporations to make their messaging services interoperable. The new law has legitimised the approach taken by Matrix. The protocol, and services built on top of it, prove at the same time that interoperable, decentralised messaging is possible.

Regulation cannot force anyone to use interoperable services - they are an enabler for work done by creators of services that are alternatives to the dominant ones. There also need to be actors - businesses or non-profits - that are able to create these interoperable services. More broadly, this is a question of whether there are

sufficient capacities and skills to benefit from interoperability - for example, whether there is sufficient technical expertise in public institutions to deploy alternative solutions, instead of simply accepting the offer of the Big Tech companies. Attention also needs to be paid to the design of interfaces - as these have a cultural role that determines adoption of services. Today, Big Tech wields social and cultural power by excelling in the design of interfaces.

And regulatory action can also have spillover effects - the introduction of the DMA has raised interest of standards bodies, for example IETF has a working group on interoperability of messaging services.

Interoperability helps market innovation and sovereignty of users

**interoperability measures
also serve to support
sovereignty**

Interoperability is often discussed solely in terms of market competition. Yet it is a principle that is generative: that can lead to broader shifts in online ecosystems. Interoperability is interesting as it makes dominant services contestable through the creation of new markets. It allows alternatives to be created, and for users to put pressure on services - since in an interoperable space there is always the risk of them switching to other services.

The Open Banking provisions, introduced in the UK, are good example of the impact of interoperability measures. Open Banking has been enforced by the UK Competition and Markets Authority, which forced the nine largest banks to agree on a series of APIs that allow competitors to access data held by these banks, based on the consent of individual customers. While the regulation has not made the banking sector much more competitive, it had a big impact on innovation and helped introduce a broad range of new financial services.

Interoperability measures also serve to support sovereignty. In the case of public institutions using Matrix-based services, the rationale for adopting Matrix is mainly to control own communication infrastructure. And similarly at individual level, choice can also translate to decisions about having more control over own communications and data.

Next steps for European interoperability policies

While attention of stakeholders has focused on the interoperable messaging mandate, the DMA includes other, specific interoperability obligations for large online platforms - these include rules for virtual assistants or browser search engines. And further, broad rules for data portability will most probably be introduced in the upcoming Data Act. These will reply to Internet of Things services and voice assistants, which will be required to ensure data portability: allowing users to move their data and change services

that they are using. The Data Act will also introduce interoperability of cloud services.

We can expect European policymakers to further pursue interoperability measures. As a rule, such measures make less sense for new types of services, for spaces of technological development that are still quickly changing. For this reason, messaging - where the core functionalities are by now clearly defined and shared by many services on the market - were a good choice for regulation.

Standardisation is a crucial factor that determines the success of interoperability measures. In the case of Open Banking, banks were forced to agree to technical standards. In the case of the DMA, the proposal to give the European Commission power to nominate technical standards did not pass. Gatekeepers will come up with their own standards, and there are not strong mechanisms in place to ensure that they secure real interoperability, and that they will be followed. ○

**civil society often lacks the -
largely technical expertise -
needed to participate in
standardisation debates**

Standards as an increasingly important mode of governance of technology

In the 1970s the European Commission faced the challenge of regulating increasingly complex technological systems. And since it lacked the capacity to define the regulation in details, it decided to delegate this task to European standardisation bodies. The standards created by these private companies were formally speaking optional - but in practice companies complied, in order to avoid risks related to the interpretation of the law itself.

Standard-setting is often framed as a technical activity, conducted away from the political debates taking place in legislative processes. Yet this is not true, and technical standards impact societies - especially when technical systems are increasingly enmeshed with social systems.

The case of the European AI Act and the growing role of standardisation

This regulatory model has been introduced by the European Commission into the Artificial Intelligence Act, which is the first digital regulation to depend so much on standards as regulatory means. And as a result matters related to fundamental rights have been delegated to standardisation bodies. In principle, standardisation is meant to ensure the regulation of high-risk AI applications, in spheres such as health, education, policing or critical infrastructure. Yet the standardisation bodies lack the sectoral expertise, and as a result are drafting standards that look the same across these spheres, and do not take into account their specificity. And there also are limits to creating public interest, society-centric rules through technical standards.

The AI Act process also shows challenges related to the participation of civil society in the standardisation work. Traditionally, public interest advocates have focused their attention on the legislative process. And they are largely missing from the standardisation bodies, which have already started work on the standards, in parallel with the legislative work. In addition, civil society often lacks the - largely technical expertise - needed to participate in standardisation debates.

This participatory challenge could to some extent be solved by engaging public standards bodies in the process. These bodies

provide greater procedural legitimacy, and also ensure openness of the standards themselves - as those created by private standardisation bodies or copyrighted, and often expensive, thus limiting their accessibility. Yet public standardisation bodies will face the same challenges with participation: few actors will have the capacity to engage in the process, and to give it legitimacy.

The standardisation bodies, and their four functions

There are four private standardisation bodies that are relevant for standard setting of the internet and related technologies: the World Wide Web Consortium (W3C) does mainly web standardisation, IEEE focuses on hardware standards, Internet Engineering Task Force (together with the Internet Research Task Force and the Internet Architecture Board) deals with standardisation of the layers of the internet that are not addressed by W3C or IETF.

Here is also the ITU, the oldest international body that is part of the UN. And while it has been attempting to play a role in internet standardisation, this approach has received a lot of push-back.

Private standardisation bodies do four things: they make standards, they deal with the governance of standard making, they deliberate on principled (as a form of long-term thinking), and they conduct cross-cutting research work and knowledge building.

The deliberation on principles is well visible in the IETF's work on AI standards. The Task Force published a document that outlined the principles for human rights focused AI development - and this framing was the result of successful advocacy of a small group of civil society actors. Alternative principles that were proposed aimed at watering down these principles - which ultimately turned out to have direct impact on standardisation processes.

Structures for participatory standard setting

The composition of the different bodies determines to what extent their process is participatory, and structures the possibility of civil society engagement in these processes. Both W3C and IEEE are membership driven. And the ITU stands out due to the fact that it is heavily state driven. In the last case, this means that the ITU has been doing important work on enabling broader access, especially through its Development Sector.

And of all these four bodies the IETF is the most open, both in terms of document sharing and the participation in the drafting process. For public interest advocates, this openness concerns not just the standardisation process, but also the other elements: work on governance, and on principles. It's easier for civil society to create its own space within the standardisation process. The Public Interest Technology Group at the IETF is an effort to create such space, with impact upon IETF that goes beyond just standards, governance or

the deliberation on principles is well visible in the IETF's work on AI standards

principles - and the group takes advantage of the fact that IETF is an open forum.

Efforts to make the IETF process more participatory don't necessarily concern standard setting. There is important work being done through talks and interventions, that provide IETF participants with new perspectives on technology. Similarly, the Global access to the internet for all research group has been established with a similar approach in mind - to shape the broader mindset of IETF stakeholders.

Challenges to open standard setting

Fora like the IETF also create space for corporate advocacy. Often a company that is developing a certain technology enters a standards body, and as a result the research and development phase becomes more open. Comments made by stakeholder groups are made public, and legitimised through the IETF process, possibly creating pressure on the company.

One of the key challenges for standards bodies are incentives that lead stakeholders to participate. The dominant reason today is market domination: parties enter these processes with the hope that a standard will be designed in a way that will enable the given company to dominate the market. While these incentives are working, they do not necessarily serve the public interest. Also, standards bodies lack mechanisms of arbitrating opposing interests of stakeholders.

While the bodies pay a lot of attention to internal governance, they in turn dismiss the issue of external governance: how they interact with other organisations, or how standards interact with regulation. W3C, if we see it as an international commons regulator, is not good at figuring out its connections with other relevant organisations and governance fora.

Standardisation work of W3C is contingent on the openness of user agents. Even with open protocols and ensured interoperability, the ecosystem can be captured by dominating the user agent market - which is beyond the scope of governance of these standardisation bodies. One solution to this would be introducing some kind of a fiduciary regime for user agents, which would define legal obligations for actions as the agent of the user, in the user's interest. Dealing with this kind of issues requires bridging gaps between standards bodies and other governance and regulatory bodies. ○

one of the key challenges for standards bodies are incentives that lead stakeholders to participate

Action points

The round-table discussion was an opportunity to assess the shifting policy terrain and possible strategies for intervention. We highlight three points to consider for policy advocates here:

1. **Standards bodies** are delegated an increasing role in European policy making as standards and certification are instrumentalised in regulation in competition and trade, as well as values and norms. The implementation of the AI Act is a case in point. Policy advocacy that traditionally targeted policy making needs to shift towards standards in order to influence outcomes.
2. **Telecommunication companies** attempt to diversify their role in digital services from providing access to data and compute provision. The introduction of smart networks such as 5G are a case in point, as well as the identification of citizens and consumers through mobile phones and SIM cards. Digital rights activists who traditionally focus on the Internet alone might want to consider widening their focus and perspectives to telecommunications.
3. The **European Parliament elections** will result in a *new European Commission* to be set up, shifting the balance of power and changing who is in charge of relevant portfolios.

Standards bodies are delegated an increasing role in European policy making

On a more close range tactical level the *Digital Markets Act*, *AI Act*, *Data Act*, *European Digital Identity (eIDAS)* and future *digital euro* processes have been mentioned in the workshop as legislative processes to especially relevant to the public interest in the ecosystem of standards and protocols.

The take-away for learning from European developments such as AI standards is that *regulating interoperability works*, highlighting the role of sovereign powers in shaping the ecosystem. European policy has knock-on effects and spill-over to other regions through leading by example, the entanglement of industrial processes, research and development, as well as markets. Centring people and planet through shifting power to the public interest can increasingly happen through standards development, governance and policy with the input of a strategically aware civil society. ○

References

- Abbate, Janet. 1999. *Inventing the Internet*. First, hardcover edition. Inside Technology. Cambridge, MA: MIT Press.
- Bratton, Benjamin H. 2015. *The Stack: On Software and Sovereignty*. Boston, MA: MIT Press.
- Cath, Corinne. 2023. "Loud Men Talking Loudly: Exclusionary Culture of Internet Governance." critical infrastructure lab report. <https://www.criticalinfralab.net/wp-content/uploads/2023/04/LoudMen-CorinneCath-CriticalInfraLab.pdf>.
- Hillebrand, Friedhelm, ed. 2001. *GSM and UMTS: The Creation of Global Mobile Communication*. Chichester: Wiley. <https://archive.org/details/gsmumtscreationo0000unse/>.
- Russell, Andrew L. 2014. *Open Standards and the Digital Age: History, Ideology, and Networks*. 1st ed. Cambridge Studies in the Emergence of Global Enterprise. Cambridge: Cambridge University Press.
- Wallerstein, Immanuel. 1991. *The Capitalist World-Economy*. Reprint. Studies in Modern Capitalism. Cambridge: Cambridge University Press.



critical
Infrastructure
lab

