Andersdotter, Amelia; Olejnik, Lukasz

Article

Policy strategies for value-based technology standards

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Andersdotter, Amelia; Olejnik, Lukasz (2021) : Policy strategies for value-based technology standards, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 3, pp. 1-26, https://doi.org/10.14763/2021.3.1573

This Version is available at:
https://hdl.handle.net/10419/245344

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Policy strategies for value-based technology standards

Amelia Andersdotter
Council of European National Top-Level Domain Registries (CENTR)
Lukasz Olejnik *European Data Protection Supervisor*

DOI: https://doi.org/10.14763/2021.3.1573

Published: 30 September 2021
Received: 10 November 2020 **Accepted:** 17 March 2021

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Andersdotter, A. & Olejnik, L. (2021). Policy strategies for value-based technology standards. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1573

Keywords: Standards, Technology policy, Accessibility, Privacy, Security, Strategy

Abstract: Formal, government-driven technology standards developing organisations (SDOs) traditionally serve as platforms for compromise between existing national standards. In the past decade, the recognition of the driving role of SDOs in innovation has made them surface into the public debate. The influence of the work overseen by non-formal, industry-driven standards bodies including the W3C, the IETF or the IEEE is increasingly acknowledged as having both direct and indirect impacts on societies, modes of work, technology policy or politics. Starting from the European Commission's formulation of "European values", we map the interplay between enforcement of codified societal norms and industry priorities.This paper identifies policy interventions that may lead to a positive influence on the development and adoption of technology standards that bring benefit to users.

This paper is part of **Governing "European values" inside data flows**, a special issue of *Internet Policy Review* guest-edited by Kristina Irion, Mira Burri, Ans Kolk, Stefania Milan.

Introduction

The relationship between policy and technical standards has seen a new role in the European Union information technology services policy (Lundqvist, 2017). Standardisation is increasingly seen as a way of ensuring that politically determined values are enshrined in technologies deployed for use by public sector institutions and citizens in areas as diverse as data protection and accessibility (General Data Protection Regulation (GDPR) Art 25; ePrivacy Directive[1] Rec. 66; Directive (EU) 2016/2102). Technical standards can be used to establish conditions under which products may be placed on a market. Technical standards can simultaneously achieve the goals of foreseeability for consumers and industry, and of protectionism (Villareal, 2018; Lundqvist, 2017) when they function as non-technical barriers to trade.

The European Union approach to harmonised standards is motivated by reducing protectionist barriers to trade. The approach dating back to 1985 is a way of establishing cross-border openness for trade inside the European Economic Area (Consilium, 1985). The approach was updated in 2012 (Regulation 1025/2012) and it consists of a set of mechanisms that allows for the European Commission to request a "harmonized European standard" (Art. 10, ibid.) for a given technical field. If the standard is completed and compliance with the standard can be demonstrated by a market actor, this harmonisation causes the products of a market actor to be presumed compliant with applicable European law and it can be traded and sold on the European inner market (Contreras, 2019). The underlying idea is to avoid the potential language barriers and regulatory costs (Villareal, 2018) associated with the emergence of national standards for entities trading within Europe while ensuring that consumers still benefit from the safety and other features that are foreseen in legislation.

This so-called new approach (Consilium, 1985; Regulation 1025/2012) of the European Union to standardisation is especially suitable for old technologies and industries (Lundquist, 2019). A standard which is harmonised through the European standards framework, consisting of multilateral cooperation platforms such as CEN/CENELEC (European Committee for Standardization / European Committee for

1. Directive 2002/58/EC on privacy and electronic communications.

Electrotechnical Standardization) or the multilateral-business hybrid organisation ETSI (European Telecommunications Standards Institute), is intended by the European legislators to find a compromise between existing national standards. Examples include safety in steel pipes, safety mechanisms in amusement devices, or resilience of electricity plugs. According to Björn Lundqvist "[i]t is an efficient way to establish 'the' technology for an industry that is already well adapted [to that technology]" (Lundqvist, 2019). However, for newer forms of technologies, the European "new approach" is struggling.

One challenge in information and communication technologies is that innovation and standardisation are often done concurrently. Namely, new products do not enter the market unless they are already standardised. As a result, these products reach end-consumers without there being national standards to reconcile, and subsequently the main purpose of the European formal standardisation procedure cannot work as intended (alternatively, it introduces a significant amount of redundancy). More recently, standardisation groups like OpenRAN, Cloud Native Computing Foundation, or the Open Handset Alliance focus on open source code and collaborative development of a single, infrastructural product, such as radio access network control software, mobile operating systems or server farm orchestration tools. This work happens without doing the initial step of standardisation at all, a choice meant to ensure the flexibility of the product (Yamany, 2019).

Section 1: Challenges ahead

In the upcoming decade more resources will be dedicated at the European and member state level towards concepts such as digital sovereignty, regulatory leadership, and state-of-the-art innovation. It is pertinent to analyse the European Union's ability and preparedness to interact with standardisation activities outside of the 'new approach' rooted in 1985. In this paper, we look at the incorporation of "European values" in technical specifications, and the ability of the European Union to absorb such values-conformant specifications into procurement, guidelines and industry. The moral leadership exhibited by the European Union in its regulatory agenda may have a tangible impact on especially informal (non-governmental) standards activities, but the incorporation of these results in practical oversight work remains precarious.

In adhering to or upholding regional norms it is not just the technical specifications that matter. The implementation of technology may carry moral weight even if the standardisation work has been questioned (Werle and Iversen, 2006). While the European Commission has the legal right to request standardisation initiatives

(Kamara, 2017) and it may be assumed that this is done with respect for European values, it is not clear that this top-down imposition of "European values" answers the question of whether there may be other ways of ensuring that digital infrastructures serve European citizens and businesses.

In this paper, we explore links between technology standards and European values. We argue that the European Union should devote more resources towards absorbing already existing innovation and standardisation into its compliance mechanisms. Not doing so would be a grave risk to policy projects such as the European strategic autonomy (Brustlein, 2018) and European digital sovereignty (Reding, 2015). Shaping standardisation with European values is only possible through the lens of a human-centric approach to technologies. Fortunately, major standardisation bodies recently place the end-users (i.e. the humans) at the centre of interest. This aligning is well evidenced by the interest in cybersecurity, privacy, but also accessibility.

We build on extensive surveys of literature, existing regulations, and strategies, as well as the practical experience of participation in standardisation activities. This multi methods approach allows us to analyse the intersection of technology, regulations, policy, and values, and to identify shortcomings of the current European approach. Our observations are intended to have immediate implications for technology policy.

We do not exclusively link to the recent experiences with the GDPR . Such as its impact on data protection evolution, including globally, outside the European Union, both on the legal frameworks (Marovic and Curcin, 2020; Petrova, 2019), as well as on technology development practices to ensure compliance (Li, Yu, and He, 2019). This success is partially due to the apparent extra-territorial application of the GDPR, an approach attempted also by the AI Regulation (Proposal for a Regulation laying down harmonised rules on artificial intelligence, 2021). The previous major success of the European technology standardisation approach in the field of technologies, the popularisation of the 2G telecommunication standard, dates to the 1990s (Tan, 2001; Gandal, Salant, and Waverman, 2003), and could only occur in a radically different technological landscape that was much more nationally fragmented than it is today. Finally, we connect some shortcomings in the current approach to technical standardisation in the EU to advances in web accessibility.

Section 2: European values and technology

Section 2.1: Values relevant to standards

The validity of the very term "European values" is often questioned (Kundnani, 2019) and has been subject to extensive exploration in literature, for example to untangle its meaning (Halman, Sieben, and van Zundert, 2011). The Charter of Fundamental Rights (Charter of Fundamental Rights, 2012) lists the following core values: human dignity, freedom, equality, solidarity, citizens' rights, and justice. The European Commission instead lists human dignity, freedom, democracy, equality, rule of law and human rights. In spite of differences there are large overlaps (The EU Values, n.d.).[2]

"European values" should, however, not be conflated with the more generic term "human rights" as enshrined in the Universal Declaration of Human Rights (UDHR, 1948). The potentially more expansive notion of European values in relation to international norms may instead have an effect on technology developers' attempts at reconciling their innovations with fundamental human values, at least in the European area. In the development of technologies aiming to function globally it might be preferable to rely by the SDOs on global values rather than regional specificities. For example such preference is seen in the Request for Comment (RFC) 8280 from the Internet Research Task Force (IETF) (IETF RFC8280, 2017), which specifically opts for a UDHR lens on human rights.

Technical standardisation is often concerned with a level of specificity not suitable for the high-level open-ended lists that function as frameworks for European policy discussions. Rather, technical standardisation can be envisaged as a tool to further European values (e.g. the list contained in Table 1 below, or similar) and policy only after the legislator has made more concrete what obligation it considers to stem from those values. A clear case is the General Data Protection Regulation (GDPR) and the associated directive on processing of personal data by law enforcement authorities (DPD) as implementations of Articles 7 (respect for private and family life**)** and 8 (protection of personal data**)** of the Charter of Fundamental Human Rights. Another case is the evolution of obligations on regulatory authorities to ensure the adaptation of electronic communication and information society services to disabled, socially exposed, or the elderly. Such acts include the Universal Service Directive (Directive 2002/22/EC), and specifications of public website accessibility requirements in the Web Accessibility Directive (Directive (EU) 2016/

2. The values list is up to date as of the retrieval date of 26 July 2021.

2102). A final case concerns the adaptations of technical solutions to nominal, but abstract, legal requirements on communication technology providers in the field of lawful interception. In this case the legislator has not specifically regulated any technical details, but through the participation of appropriate law enforcement authorities in standardisation processes the technology is still shaped by invocations of laws on the book.

Section 2.2: European values linked to technology

While many potential links between technical standards and European values may be identified, we focus on a few specific examples of relationships to privacy, data protection, accessibility and non-discrimination. These rights are linked to both human rights and equality. To some extent also freedom (especially where it concerns usability of information society services) and even human dignity, when sensitive data is shared, processed, or made available in various formats with respect to accessibility. The central aspects of these laws are clearly linked to technology and technology standards. The legal realm (COM (2015) 615 final; Directive 2016/2102) as well as the technical aspects of assistive technology may be a practical emanation of the rights of the elderly or non-discrimination with respect to disability, both clearly linked to human dignity (Borg and Östergren, 2011).

Assistive technologies and accessibility are already within the interest of technology standards bodies such as the W3C and the IETF. The notion of European value of dignity, closely related to "non-discrimination" and the "integration of persons with disabilities" is naturally relevant to technologies and standards. This importance is evidenced by the focus on accessibility in technology layers (Web Accessibility Interest Group, n. d.; Internet Society Accessibility Working Group, 2019). Finally, assistive technology is also mentioned and their design, creation, and use explicitly promoted in the United Nations Convention on the Rights of Persons with Disabilities (The Convention, 2016, Article 4(g)).

It is likewise straight-forward to appreciate the importance and relevance of the protection of personal data to the end users, as evidenced with the spike of interest in societal and technical aspects of data privacy (W3C Privacy Interest Group, n. d.; IETF Privacy Enhancements and Assessments Research Group, n. d.; IEEE 802E Recommended Practice for Privacy Considerations for IEEE 802 Technologies, n. d.). Indeed, as of today all standardisation bodies have a clear interest and dedicated working groups devoted to privacy (IETF's Privacy Considerations for Internet Protocols, 2013) or cybersecurity (W3C's Web Application Security Group, n. d.). The IETF, for example, understands its position as the key stakeholder responsible for

internet privacy (Peterson, Tschofenig, Aboba, and Sollins, 2010).

Section 3: How standardisation works

Section 3.1: Standards body mechanisms

The work of standardisation bodies may be very complex (Lazanski, 2019) but from the point of view of our assessment most standardisation bodies follow a similar basic fundamental mode of operation. The practical work involves individuals representing themselves, public or private institutions, or companies. These individuals work in groups to produce deliverables that are subsequently developed and accepted as standards. The delivered standards may be made accessible to implementers for a fee, or publicly without charge. They are voluntary for industry players to implement in whole or in part, but can be used to ensure interworking with products of other manufacturers or to demonstrate compliance with regulatory requirements. While differences exist across standardisation bodies, this broad and simplified description generally holds and is sufficient for our considerations.

Standard deliverables may take a variety of forms. Soft deliverables such as methodologies for assessment or checklists may be called process standards. The ISO 27000 series related to information security is a widely used standard for information security that adopts this approach. Similar examples of other standardisation bodies include IETF Best Current Practice documents or W3C Web Content Accessibility Guidelines 2.0. Standards may describe a technology concept such as the behaviour of specific networking protocols or other. Examples include the Hypertext Markup Language (HTML) used to design websites (World Wide Web Consortium, HTML 5.2), or the specification for privacy-aware IPv6 address generation (IETF RFC4941).

Decisions about the features going into standards and which features are being left out have real consequences for technologies and processes that are used by millions to billions of users. Similarly, inclusion or exclusion of features can tangibly impact anything from what business model can be applied by using the specified technology, to the technology's conduciveness to add-on innovations. This framework of influence makes it important to appreciate several points. Those aspects include who (in principle) should be empowered to make such decisions, how the making of such decisions can be legitimised, to what extent the decisions are influenced by or interact with norms established through the usual norm-setting processes of societies (in the European Union, typically through legislation, regulation, and democratically elected bodies), and lastly, whether standards

should conform to any predefined moral framework external to the standards body itself, such as the moral framework enshrined in law. Technology standards are in fact not neutral from a values perspective and this gives rise to the question of whether these should consciously refer to any specific set of values (Brown, Clarkand, and Trossen, 2010; ten Oever, 2020).

Technologies tend to be impacted by indirect, extrinsic norms. For instance when certain market behaviours are incentivised by legislation, which in turn causes innovations in directions that make that behaviour easier, including the adaptation of business models. This way, even the "Internet can be made to treat censorship as a feature, not a bug" (Boyle, 1997). To understand this point and to appreciate its strong relevance to specific sets of values that technologies may conform to, it suffices to reference the longstanding debate about strong encryption, where various stakeholders hold starkly different opinions. Technology circles have long favoured strong cryptography (Global Encryption, 2020), while some state authorities are increasingly skeptical and critical (U.S. Department of Justice, 2020). Authorities of various states argue that it is important to be able to reverse encryption for law enforcement or national security purposes. Skepticism can also manifest in the active state-wide blocking of technologies like the Transport Layer Security (version 1.3) that does not support bypassing of strong confidentiality guarantees (Bock et al., 2020). Business groups also identify reasons to protest advancements of more robust end-to-end encryption practices (O'Neill, 2018). States may also consciously show lenience with standardisation bodies or private sector entities that do not implement correct security patches when flaws are discovered (Pell and Soghoian, 2014).

Section 3.2 The place of values in technology

While the IETF and the W3C are catering to different communities of technology developers, they are remarkably in agreement with respect to the priority of constituencies in future applications of standards. In particular, both bodies give priority to the end-user. The IETF goes as far as to say that "when there is a conflict between the interests of end users of the Internet and other parties, IETF decisions should favor end users'' (The Internet is for End Users, 2020). Similarly bold declarations can be found in the core W3C design document (HTML Design Principles, 2007). It states that "[i]n case of conflict, consider users over authors over implementers over specifiers over theoretical purity". Such framings of priority open the interpretation of decisions with consequences to technical concepts like privacy, security, flexibility, reachability in favour of users. We reflect that this focus on the end-user—specifically the human—is a vehicle which lends itself to shaping tech-

nologies with human dignity, and more generally with human rights and values.

There is strong and legitimate criticism against explicit connections between technology standards and legal values (Mueller and Badiei, 2019). However, we point out that this connection is already a practical reality. Moreover, it has strong historical precedence, for instance in cases where technology standards are used to facilitate free trade (we return to this point below). The link between values and technologies is assumed in formal standardisation organisations (such as ETSI, CEN/CENELEC, ISO) in order to accommodate for geopolitical and corporate diversity. The European framework for formal standards expressly revolves around the realisation that technical standards are used to achieve industrial policy goals (for example, they can be used to maintain non-tariff barriers to trade between EU member states). Examples from the mobile networking space are well-studied (Taylor, 2019, Meier-Hahn, 2015, Pell and Soghoian, 2014), and the Clean Network policies enacted by the US State Department in 2020 illustrates the growing politicisation of technical standardisation even further. Links exist also in other areas such as sustainability, where technical standards that assume policy goals are energy classifications for electrical equipment (for example, motivated to counter global warming) or consumer protection features such as maximal decibel rates in headphones (motivated with protecting people's health).

In the field of data protection, the incorporation of data protection by design (also known as privacy by design) and by default as legal obligations on users of technologies (GDPR, Art. 25) is a most notable example of normative thinking around technologies. This policy is meant to shape how technology is used, created, or designed.

An earlier case is the engagement of US and EU public authorities in Do Not Track mechanisms at the W3C. The W3C Do Not Track standard (Tracking Protection Working Group Charter (disablement of the group), 2019; Safari 12.1 Release Notes (removal of Do Not Track), 2019; A Second Life for the 'Do Not Track' Setting—With Teeth, 2020) is a less successful example of values shaping technologies. In spite of a European law enacted to specifically encourage the type of privacy-protections planned for development in this working group (Directive 2009/136/EC, Art 3.5), the endeavour did not successfully engage industry, policymakers, or the public. It was widely acknowledged that the differing approaches to privacy on the web between the European Union and the United States created a lack of clarity both on the scope and goals of the standardisation project. The ensuing lack of engagement by European entities charged with upholding the values incorporated in the body of European law did not contribute towards a successful outcome. Nei-

ther the European data protection authorities nor other regulatory bodies participated in the development of the standard, with the result that the practical manifestation of European law in technology remained unclear. Industry players could not satisfy themselves that the standard under development would be helpful in achieving conformance.

Inclusion of privacy at the design phase of technologies is a positive example of cooperation between regulation and technologies. The case of Do Not Track is a negative example of what happens when technology and policy do not work in sync. These real-world technology policy examples highlight that furthering the case for values in technology design relies not only on legal text, but also on regulatory backing. In other words, merely enacting values-based frameworks to shape technology (Manders-Huits, 2011), or similarly, merely designing the technologies without policy backing, is not enough. Such an approach may indeed be limited (Mueller and Badiei, 2019). We understand and acknowledge that active policy backing is a necessary component—and in fact also at play in notable policy standardisation organisations such as ICANN (ICANN GAC, Europol EC3 ICANN engagement initiative) and the 3GPP (3GPP-SA3-LI) or, more recently, RIPE (e.g. RIPE NCC MoU with Europol). In these latter examples, there is not even a need for a specific legal basis for the influence of values on standards. Rather, they exemplify how values incorporated in the body of law can exercise indirect influence on technical standards and their implementations.

Existing institutions and market actors operating inside of a regulatory framework that predates the development of technologies, will see their interests challenged by technical developments and engage with a view to better understanding and shaping technologies to serve their existing operational mechanisms. Removal of harmful or illegal content is one of the more notable areas where values have shaped technology, in fields ranging from the domain name system to online platforms. The pre-existing obligations on financial institutions to monitor transactions also created an indirect need to try and influence the creation of more robust encryption standards for internet-based data traffic (Patrick Howell O'Neill , 2018).

TABLE 1: Example cases of links between policy, technologies and standards

CONCEPT	POLICY INTERVENTION	EFFECTS ON TECHNOLOGY
Access to telecommunication content	National laws	Ensuring lawful intercept capabilities in telecommunications

CONCEPT	POLICY INTERVENTION	EFFECTS ON TECHNOLOGY
		networks by influencing the use of encryption in hops between networks, or the use of identifiers inside of networks.
Accessibility	EU Web Accessibility Directive	Upholding of W3C WCAG. Technologies and websites designed with disabled in mind. Assistive technologies.
Do Not Track (DNT) signals	ePrivacy Directive	Used to be considered a pathway to regulatory compliance, also within the EU. Now with diminishing support and legal clarity.
On-demand operating system modifications	French policymaker pressure (contact tracing)US requests of iOS unlocking in judicial probe	No effects.
Privacy in the design phase	GDPR and laws modeled on it	Privacy considered on the design phase of technologies and standards. Standardisation checklists for privacy considerations influenced on activities in basic communication standards at organisations like the W3C, IETF, and IEEE. Impact on how identifiers are constructed (i.e. to limit privacy risks of fingerprinting), or the amount of attention paid to security work while

CONCEPT	POLICY INTERVENTION	EFFECTS ON TECHNOLOGY
		completing the standard.
Reversible encryption / on-demand decryption	(Predominantly) national laws	Impact on integrity and confidentiality of elements in communications technologies or web services (i.e., delayed improvements, fewer safeguards against flaws, etc.).

Section 3.3: Politics impacts on technology

We stress that the presence of politics in the technology sphere is already a reality. We offer two concrete examples of policy-based interventions in technical design from the fields of cryptography and the Covid-19 crisis response (digital contact tracing).

In 2016, a California court ordered Apple to modify its operating system for law enforcement purposes in a case that eventually brought the interest of the entire world (Kim Zetter, 2016). In this case, Apple argued that to compel them to modify the operating system would infringe freedom of speech, as it would necessitate the modification of the operating system source code (Laura Sydell, 2016).

In 2020, French politicians tried to convince Apple to modify its operating system in order to allow the pursuit of French sovereign ideas for digital contact tracing applications (Fabienne Schmitt and Florian Dèbes, 2020). Notably, those politicians referred to the concept of technological sovereignty.

So far these attempted interventions have been unsuccessful. But the complexity and variety of the listed examples highlight the already existing relationships between politics and technology, either as new technologies clash with old policies, or as policymakers attempt to influence old technologies by increasingly complex new policy frameworks, with a list of example cases mentioned in this paper listed in Table 2. With the regulatory interest in technological developments increasing around the world, we can expect to see stronger direct relationships developing between regulatory bodies and standards bodies.

Section 3.4: Needs for regulator-standards body cooperation

The vast majority of standards bodies that work on electronics, networks, or web technologies are industry-driven consortia, with more or less formalised rules of participation. These consortia work on everything from web authentication technologies, web payments technologies, to real-access memory chips, cryptographic protocols for internet traffic, and radio network technologies.

While these consortia are successful in bringing industry actors together around a specific set of base features required for each technology, they partially lack legitimacy. The free trade frameworks established by the World Trade Organization or other bi- or plurilateral trade agreements frequently reference the role of international standard in facilitating trade, yet the process for designating a standard as "international" is elusive (Wolfrum and Stoll, 2007).

In practice, however, there seems to exist a form of implicitly accepted agreement that international standards are those which are endorsed by formal standardisation bodies that operate on a multilateral basis, such as the ISO, IEC (International Electrotechnical Commission), and ITU (International Telecommunication Union). For standards that are developed by industry-driven consortia (like the IETF) to gain international legitimacy under the global trades framework, they may need to be accepted by one of these legitimised bodies as a formal specification.

The formal international standardisation bodies are based on a multilateral principle. Industry-driven consortia can only be represented therein by country delegations consisting of individuals representing the entities participating in the consortia. Country delegations often enjoy the support of their local government administrations, creating in this sense an intermixing of regulatory bodies and standardisation bodies.

An example of national delegations clashing in the pursuit of having industry-developed standards recognised as international standards is a conflict relating to security in wireless local area networks (WLAN) between the United States and China since 2007. An early industry-developed security standard for WLAN called WEP, which ensured encryption between the client and the router, was demonstrated early on to suffer from security flaws. A Chinese competing standard, WAPI, was developed in 2003 and put forward for consideration by the international community. However, contention around the cipher suite used to support WAPI cast doubts on its robustness, and while it was originally intended to replace a flawed WEP, yet other competing standards, again developed by industry-driven

standards bodies (WPA and WPA2) ended up replacing WEP as the preferred WLAN security mechanism (WLAN Authentication and Privacy Infrastructure, n.d.).

Section 4: Challenges in the current European approach

Section 4.1: Non-flexibility of the new approach

The European "new approach" to harmonising standards between different EU member states is faced with challenges when it concerns the development of information and communication technologies. Where standardisation and innovation go hand in hand and happen simultaneously, and interoperability between different corporate and national solutions remains crucial, the European system of seeking a compromise between established national solutions is no longer optimal.

This lack of adaptability in the European framework for recognising standards was highlighted in the review of the General Framework of European Standardisation Policy (Regulation 1025/2012) finalised in 2012. Legislators acknowledged that there was no legal way of invoking a technical standard from an industry-driven consortium in a call for tender in a way that the standard would guarantee conformance with legal obligations incumbent on the deployer or manufacturer. This situation was remedied by the introduction of a multi-stakeholder platform for ICT standardisation (ICT MSP) that has subsequently gone on to recommend standards from both the W3C and the IETF, as reflected in the extensive list of Commission Decisions based on the ICT provisions of the general framework regulation (ICT technical specifications, n. d.).

Perhaps a more curious case of adaptation to technical standards from industry-driven standards in development bodies can be found in the case of the Web Accessibility Directive (Directive 2016/2102, 2016). Broadly based on the Web Content Accessibility Guidelines (WCAG) standard, which was initiated by the W3C in 2008, the Directive contains obligations on public sector institutions to ensure certain accessibility features accommodating for functionally variant individuals. The directive is enforced by a harmonised European standard (ETSI EN 301 549 V2.1.2). Therefore the path of standardised accessibility for websites in the European Union looks as follows. Informal standardisation in private standards development bodies is followed by the public law in line with the developed standard. Only after this process an implementing order is issued to formally re-standardise the pre-existing standard. This process is lengthy. A lead-time of ten years, including a full legislative process, is a significant toll given that national regulatory bodies for

electronic communications already had the competencies to ensure accessibility within the meaning of web accessibility under the updated telecoms package from 2009 (in particular the Universal Service Directive 2002/22/EC as amended in 2009).

This case also illustrates a link between an existing European value (human dignity, human rights) and a specific technical standard already developed (WCAG 2.1). Challenges remain in ensuring adoption and uptake of the European-valued specification, but similar challenges abound in other domains.

In the field of data protection, it is even less clear that the European Union can speedily absorb industry-driven developments in a way that ensures regulatory certainty. The Radio Equipment Directive (Directive 2014/53/EC) specifies that radio equipment placed on the European market should, as an essential requirement, fulfill data protection and privacy protections (2014/53/EU, Art. 3.e). In spite of this rule having been present in European law since the 1990s, a concrete specification of what this entails remains absent. Effectively, any radio equipment with arbitrary properties could potentially be fulfilling this essential requirement which would undermine the values underlying the lawful obligations. Recent attempts at mapping the needs for privacy requirements for specific sets of products (Delegated act pursuant to Articles 3(3)(e) [and 3(3)(f)] of the Directive 2014/53/EU, 2019) may finally fill in the void.

Under the current European approach to standardisation, the mechanism for specifying such requirements would consist of the European Commission issuing a standardisation mandate to ETSI, which would then be voluntary for an ETSI working group to complete. This presents the challenge of the European general framework for standardisation requiring privacy-friendly features to be in fact standardised twice before they can be invoked for regulatory compliance. Such sub-optimal resource allocation, needlessly delays adoption of societally useful technologies.

Certification according to standards was also specifically incorporated as a mechanism in the GDPR (GDPR Art. 42-43), but crucially the pathway for an industry-driven standard to be used for compliance purposes is highly unobvious. A standard would have to be endorsed by a public institution at either the European or national level (in line with the GDPR Art. 42.1), and compliance with the standard enforced by an independent certification body that would have to accept a high level of liability for its enforcement (GDPR Art 43.4), while liabilities on the certified entity under the regulation continues to remain at the same level as before the certification procedure (GDPR Art 42.4). The economic incentives envisaged by the leg-

islator for industry entities to adopt these practices remain elusive, and they would appear best suited for the type of standardisation framework that is present in the formal bodies (CEN/CENELEC and ISO in particular).

The GDPR foresees a place for the active involvement of industry players in defining their own data protection norms that preserve the high levels of data protection mandated by the law. At the same time industry players lack the mandate (or legitimacy) to establish what these norms should be. The specific interpretation of norms codified in the GDPR is subject to decisions by data protection authorities in the EU member states and ultimately the Court of Justice of the European Union. Subject matter experts in protocol, web browser, or radio technology design are not legal experts and may not be helped by high-level process standards for assessing data protection features when developing new technologies. They could be assisted by templates that are developed for the purposes of helping standards development in their respective organisations (IETF RFC 6973; IEEE P802E). However, the European Union lacks an established mechanism for working with tools to facilitate the assessment of industry-driven data protection standards. In the best case, this means that the uptake of privacy-friendly solutions is slowed down. In the worst case, initiatives for developing new privacy-friendly technologies through the help of guidelines may fail.

Section 4.1: Unfitness of the European model?

The general European framework for standards creation remains structured for facilitating interactions with international standards bodies such as the ISO, IEC, and ITU. By consolidating positions regionally, the European Union can theoretically represent a more cohesive approach in international bodies. In practice, however, 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. Particularly in radio network technologies, regional cohesion is not limited to ETSI and CEN/CENELEC, but also involves the European Conference of Postal and Telecommunications, a spectrum management organisation whose positions end up forming the basis for European work in the ITU.

The apparent failure of the W3C Do Not Track effort highlights the shortcomings stemming from the lack of European coordination, unity, and ability of rapid work. The EU continues moving at a slow pace while the outside efforts accelerate, for example in adapting to a proposed shift of internet standardisation from established informal standards bodies such as the IETF to the formal standards body ITU (China and Huawei propose reinvention of the internet, 2020; CENTR Tech

Trends Watch Q1/2020; ITU SG 13, 2017). Even beyond the European values of human rights and human dignity, it is notable from the perspective of digital sovereignty that the proposed changes to internet traffic mirror developments that have already happened within the IETF working groups (IETF DETNET, IETF RAW, IETF NVO3, IETF RFC 8799) and in the 3GPP (3GPP TS23.682), where European-based companies are taking the lead in technical development and standardisation. With stark warnings of these attempts precipitating the fragmentation (balkanisation) of the internet itself (Hoffmann, Lazanski, and Taylor, 2020), it remains unclear how the European Union will balance its diverse industrial interests with its equally diverse European values.

Meanwhile, technology standards are a solid vehicle for the advancement of both industrial (Harbour & Bjerkem, 2020; Lundqvist, 2017) and societal interests. This is reflected in legislation covering areas as diverse as data protection and eco-labeling, but also in the commitment of the European Union to ensure the representation of a broad range of stakeholders in formal standards procedures. Consumer organisations, environmental organisations, and labour unions can participate in the process that leads up to a harmonised European standard, often with financial contributions from the European institutions themselves to ensure continuity.

However, the informal standardisation processes, which define the information and communication technology landscape even as it is adapted to the European formal standards procedures, remain without diverse representation. Not only is there a lack of institutional representation in industry-driven standards organisations, as was the case in the W3C Tracking Preferences Expression endeavour. There is also a lack of diverse representation within the meaning of European formal standards processes. Traditionally groups such as consumer representatives, environmental groups and labour unions have been allocated specific grants and resources to ensure European values are manifested in the formal technical standards works undertaken by formal standards institutions (Regulation 1025/2012 1025/2012 Annex III, 2012). But these diversification groups are not resourced to ensure the same level of European values in the informal technical standards work undertaken by industry-driven consortia.

Section 5: Policy recommendations for the road ahead

In this article, we identify a puzzle. Technology and standards are increasingly instrumental in politics and policy, and policy exerts influence on technologies. We shed light on the links between human rights and European values, and the relationship to European Union standardisation policy and technology standards. We

highlight the limitations of the (in fact old) European "new approach" to harmonised standards and propose three policy directions.

First, the European Union must simplify the current policy of re-standardising the already accepted standards developed by other stakeholders, at least in industries where standards are developed by industry stakeholders at the global level rather than by national bodies covering national industries (Lundqvist, 2017). The formal standardisation rules currently in place are useful when compromise is needed between national bodies with established procedures, but hinder the ability of the European Union to absorb—that is, to accept and give a legal backing—to technology standards in the ICT space. In a world where voluntary standards organisations play an important role, such a technology policy unnecessarily slows down the pace of aligning legal norms with technical norms. European citizens may also be left without valuable technological advancements. A first step has been taken through the establishment of the ICT multi-stakeholder platform (ICT MSP) initiated in the previous standardisation reform in 2012. However, this group has not approved any new standards since 2017 and the uptake of ICT MSP approved standards by procuring authorities remains unclear. The European Commission needs, specifically, to speed up and follow up on approval of industry-developed standards by procuring authorities. Coordination between existing European Commission projects such as Interoperability solutions for public administrations, businesses and citizens (ISA2), JoinUp and ICT MSP may also be a first step to finding gaps and opportunities.

Among the challenges is that European industry players are already themselves spread out thinly over the existing industry SDOs. They currently duplicate efforts of national, regional, and international standards bodies, where international standards bodies are the most crucial for long-term success. In a regulatory risk setting, European companies also simultaneously juggle national, regional and international norms and values, all of which may or may not have an impact on the technical decisions they need to make when designing and implementing new features in products. At the same time, public authorities from EU member states are similarly spread out over several institutions, with different European states attributing different levels of importance to formal and informal standards development depending on their national economic and industrial situation. A key step in simplifying procedures is for executive authorities at the European and national levels to come together in decisions on how to deal with this mix of public and private institutions spread out over other public and private institutions in the standardisation and procurement space.

Other simplification measures could consist of relying less on formal certification and certification bodies, and more on self-certification initiatives. Self-certification could allow industry players to assess their conformance with an industry-developed norm for privacy protection, subject to hefty penalties if the assessment does not hold up to scrutiny. It would allow industry players to immediately implement a finalised industry standard. It also reduces administrative overhead and reduces the reliance of industry on EU member state-approved certification bodies. Current mechanisms under the GDPR (codes of conduct (Art. 40-41) and certification (Art. 42-43)) both foresee the creation of new institutions and administrative procedures that can be approved by public authorities to ensure e.g. privacy protection. A simplified mechanism could allow public authorities to use industry-developed norms directly to hold companies to account, without industry players coming together in a new institution designed to be scrutinised in advance of applying the norms. One way of procedurally accomplishing this without major legal overhauls of existing rules would be to involve data protection authorities closer in the work of the ICT MSP or ISA2 initiatives on public procurement efforts.

Second, the European Union needs a modern strategy of involvement in technology standards. Just like technology policy, technology and standards are not neutral (Delvenne and Parotte, 2019). The US virtually created the internet itself and maintains an influence over the technical internet architecture through powerful American technology companies in spite of the lack of an official state approach to technology policy (Branscomb, 1992). The Chinese medium-term technology standardisation plan (China Standards 2035 and the Plan for World Domination, 2020) is a recent example of a state prioritising technology standards as a strategic area of interest, while the European influence on 2G standardisation is today all but forgotten. Even the modest impacts of the European approach to accessibility on W3C's accessibility standards (Directive 2016/327; Web Content Accessibility Guidelines adoption in Europe, 2018; ETSI's Accessibility requirements for ICT products and services, 2018) highlight the links between standardisation and policy. But in the case of advancing European values, the potential to impact standards today remains unfulfilled, at least in the ICT space. Ultimately, we believe that the European Union must create its dedicated, independent, long-term and resilient approach to technology standardisation. Such EU involvement would naturally need to be grounded in EU values. The European Union could leverage existing initiatives such as the ICT MSP, ISA2, JoinUp and Open Source Observatory (OSOR) to accomplish this sort of technology standardisation. Successful scoping and mapping exercises for use and deployment of open source tools in public sector institutions already exist; similar scopings and mappings could be done for industry-

developed standards.

Third, the European Union must realise how to practically structure its influence over technology standards. Applying values via technology policy to shape innovative technologies is challenging (Van Oudheusden, 2014). In technology standardisation this is even more clear since the composition of working groups within the technology standards organisations follows a totally different model than in elective democracies. This highlights the importance of early and consistent but also long-term involvement. Promoting activities of this kind would require a policy of inducing participation from individuals or organisations well-positioned to analyse proposed technology standards with European values in mind. The policy of active participation should build on a strong understanding of how standards, technology, and technology assessment (Banta, 2009) operate, including in specific domains such as security, privacy (Olejnik, Englehardt, and Narayanan, 2017; Sion, Van Landuyt, and Joosen, 2020), accessibility or even broader like in the case of human rights assessments (Mantelero, 2018). Such a policy must encompass the adaptation of the regulation 1025/2012 on the European standardisation (Regulation 1025/2012). Promoting the active participation of European stakeholders might be achieved by extending the reach of Article 16 ("Financing of other European organisations by the Union") to the financing of non-governmental organisations or even private individuals involved in technology standards work. The recent active investment in civil society participation in industry-driven standardised processes by the US State Department (e.g., US State Department NOFO SFOP0005493; US State Department NOFO SFOP0006453) may serve as an example of such an approach in practice, one that the European Union is lacking. Motivating the European data protection authorities or standardisation oversight bodies to play a more active role may be another goal, for instance by crystallising economically tractable mechanisms for the application of the General Data Protection Regulation with its articles 42 ("Certification") and 43 ("Certification bodies") that outline the legal aspects of the data protection certification framework.

Conclusion

Human, moral, and European values are clearly linked to technology. These links are well reflected in the literature and the public debate. We identify shortcomings and gaps in the European policy approach to technology standardisation. These might be the reasons why the current approach to standardisation in Europe is no longer as effective as it was when Europe was able to popularise standards in telecommunications, such as 2G (Tan, 2001; Gandal, Salant, and Waverman, 2003).

We consider three ways forward. First, Europe should develop a consistent and long-term strategy of activity in the area of technology standards. Such a strategy should have sufficient funds allocated. Second, Europe should strengthen the technology standards (directive/regulation), simplifying the absorption of certain voluntary standards. Third, Europe should become more assertive in the area of technology standards, working towards creating a momentum of action in the standards venues. Such action should be driven by proper values. Likely, a dedicated technology standards unit or agency must oversee or drive the activities. Such an agency should not be tasked with any particular enforcement tasks. Rather, it should focus on oversight, research, development, design, and coordination of activities with the EU member states.

References

Abou-Zahra, S. (2018). WCAG 2.1 Adoption in Europe [Blog post]. *W3C Blog*. https://www.w3.org/blog/2018/09/wcag-2-1-adoption-in-europe/

Apple, Inc. (2019). *Safari 12.1 Release Notes*. Apple Developer Documentation. https://developer.apple.com/documentation/safari-release-notes/safari-12_1-release-notes

Banta, D. (2009). What is technology assessment? *International Journal of Technology Assessment in Health Care*, *25*(S1), 7-9,. https://doi.org/10.1017/s0266462309090333

Barrios Villarreal, A. (2018). *International Standardization and the Agreement on Technical Barriers to Trade*. Cambridge University Press. https://doi.org/10.1017/9781108591348

Bock, K., iyouport, A., Merino, L.-H., Fifield, D., Houmansadr, A., & Levin, D. (2020). *Exposing and Circumventing China's Censorship of ESNI, censorship.ai*. https://geneva.cs.umd.edu/posts/china-censors-esni/esni/

Bock, K., iyouport, Anonymous, Merino, L.-H., Fifield, D., Housmansadr, A., & Levin, D. (2020). *Exposing and Circumventing China's Censorship of ESNI*. censorship.ai – Geneva. https://geneva.cs.umd.edu/posts/china-censors-esni/esni/

Borg, J., Larsson, S., & Östergren, P. O. (2011). The right to assistive technology: For whom, for what, and by whom? *Disability & Society*, *26*(2), 151-167,. https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1080%2F09687599.2011.543862

Boyle, J. (1997). Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors. *U. Cin. L. Rev*, *66*, 177.

Branscomb, L. M. (1992). Does America need a technology policy. *Harvard Business Review*, *70*(2), 24-31,. https://hbr.org/1992/03/does-america-need-a-technology-policy

Brown, I., Clark, D. D., & Trossen, D. (2010). Should specific values be embedded in the Internet architecture? *Proceedings of the Re-Architecting the Internet Workshop*, 1-6 ,. https://doi.org/10.1145/1921233.1921246

Brustlein, C. (2018). European strategic autonomy: Balancing ambition and responsibility. *Éditoriaux de l'Ifri*, *16*. https://www.ifri.org/sites/default/files/atoms/files/brustlein_european_strategic_autonomy_2018.pdf

Carpenter, B., & Liu, B. (2020). *Limited Domains and Internet Protocols* (Request for Comments No. 8799). Internet Engineering Task Force. https://datatracker.ietf.org/doc/rfc8799/

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

CENTR Tech Trends Watch Q1/2020. (2020). Council of European National Top-Level Domain Registries. https://www.centr.org/library/library/other/centr-tech-trends-watch-q1-2020.html

Charter of Fundamental Rights of the European Union, Pub. L. No. C 326/391 (2012).

Commission delegated regulation pursuant Articles 3(3)(e) [and 3(3)(f)] of the Directive 2014/53/EU on internet-connected radio equipment and wearable radio equipment. (2019).

Commission Staff Working Document: Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the approximation of the laws, regulations and administrative provisions of the Member States as regards accessibility requirements for products and services—SWD/2015/0264 final—2015/0278 (COD. (n.d.).

Contreras, J. L. (Ed.). (2017). *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*. Cambridge University Press.

Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., & SmitH, R. (2013). *Privacy Considerations for Internet Protocols* (Request for Comments No. 6973). Internet Engineering Task Force. https://datatracker.ietf.org/doc/rfc6973/

Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards (1985, Official Journal C 136, 04/06/1985 1 (1985).

Delvenne, P., & Parotte, C. (2019). Breaking the myth of neutrality: Technology Assessment has politics, Technology Assessment as politics. *Technological Forecasting and Social Change*, *139*, 64-72,. https://doi.org/10.1016/j.techfore.2018.06.026

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive, 51 (2002).

Directive 2009/136/EC of the European Parliament and of the Council of EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), (2009).

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive, (1999).

Directive 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (Text with EEA relevance. (n.d.).

Directive 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance). (n.d.).

Draft report of Marju Lauristin on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)). (2017).

ETSI. (2018). *Accessibility requirements for ICT products and services* (Technical standard EN 301 549 2 1 2). European Telecommunications Standards Institute.

Gandal, N., Salant, D., & Waverman, L. (2003). Standards in wireless telephone networks. *Telecommunications Policy*, *27*(5–6), 325-332,. https://doi.org/10.1016/S0308-5961(03)00026-0

Gross, A., & Murgia, M. (2020, March 27). China and Huawei propose reinvention of the internet. *Financial Times*.

Halman, L., Sieben, I., & Zundert, M. (Eds.). (2011). *Atlas of European Values. Trends and Traditions at the turn of the Century*. Brill.

Harbour, M., & Bjerkem, J. (2020). *Europe as a global standard-setter: The strategic importance of European standardisation* [Discussion Paper]. European Policy Centre. https://www.epc.eu/en/Publications/The-strategic-importance-of-Europe~37f244

Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: How China's technical standards could fragment the internet. *Journal of Cyber Policy*, *5*(2), 239-264,. https://doi.org/10.1080/23738871.2020.1805482

Huawei Technologies. (2019). *Internet 2030—Towards a New Internet for the Year 2030 and Beyond* [White Paper]. International Telecommunication Union.

IEEE 802E Recommended Practice for Privacy Considerations for IEEE 802 Technologies. (n.d.).

Internet Society Accessibility Special Interest Group. (2020). https://www.a11ysig.org/

Internet Society Open Letter Against Lawful Access to Encrypted Data Act. (2020).

Kamara, I. (2017). Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology*, *8*(1).

Kundnani, H. (2019, April 22). EU's two-faced 'values'. *Politico*. https://www.politico.eu/article/eu-two-faced-values-rule-of-law/

Laboris, I. (2019). *The impact of the GDPR outside the EU*. Lexology. https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f

Lazanski, D. (2019). Governance in international technical standards-making: A tripartite model. *Journal of Cyber Policy*, *4*(3), 362-379,. https://doi.org/10.1080/23738871.2019.1696851

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1). https://doi.org/10.1080/1097198X.2019.1569186

Lundqvist, B. (2017). Standardization for the Digital Economy: The Issue of Interoperability and Access Under Competition Law. *The Antitrust Bulletin*, *62*(4), 710–725. https://doi.org/10.1177/0003603X17733359

Lundqvist, B. (2019). Public Law, European Constitutionalism and Copyright in Standards. In J. L. Contreras (Ed.), *The Cambridge Handbook of Technical Standardization Law* (1st ed., pp. 124–142). Cambridge University Press. https://doi.org/10.1017/9781316416785.008

Manders-Huits, N. (2011). What values in design? The challenge of incorporating moral values into design. *Science and Engineering Ethics*, *17*(2), 271-287,. https://doi.org/10.1007/s11948-010-9198-2

Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, *34*(4), 754-772,. https://doi.org/10.1016/j.clsr.2018.05.017

Marovic, B., & Curcin, V. (2020). Impact of the European General Data Protection Regulation (GDPR) on Health Data Management in a European Union Candidate Country: A Case Study of Serbia. *JMIR Medical Informatics*, *8*(4). https://doi.org/10.2196/14604

Meier-Hahn, U. (2015, December 17). Cogent v Deutsche Telekom: A classy conflict. *Internet Policy Review*. https://policyreview.info/articles/news/cogent-v-deutsche-telekom-classy-conflict/393

Mueller, M. L., & Badiei, F. (2019). Requiem for a dream: On advancing human rights via internet architecture. *Policy & Internet*, *11*(1), 61-83,. https://doi.org/10.1002/poi3.190

Narten, T., Draves, R., & Krishnan, S. (2007). *Privacy Extensions for Stateless Address Autoconfiguration in IPv6* (Request for Comments No. 4941). Internet Engineering Task Force. https://datatracker.ietf.org/doc/rfc4941/

Nottingham, M. (2020). *The Internet is for End Users* (Request for Comments No. 8890). Internet Architecture Board. https://datatracker.ietf.org/doc/rfc8890/

Olejnik, L. (2019, February 28). A Second Life for the 'Do Not Track' Setting—With Teeth. *Wired*. https://www.wired.com/story/a-second-life-for-the-do-not-track-setting/

Olejnik, L., Englehardt, S., & Narayanan, A. (2017). Battery Status Not Included: Assessing Privacy in Web Standards. In *IWPE@ SP* (pp. 17–24).

O'Neill, P. H. (2018). Big banks want to weaken the internet's underlying security protocol. *CyberScoop*.

Pell, S. K., & Soghoian, C. (2014). Your secret stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy. *Harv. JL & Tech*, *28, 1*.

Petrova, A. (2019). *The impact of the GDPR outside the EU, Ius Laboris/Lexology*. https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f

Proposal for a Regulation laying down harmonised rules on artificial intelligence. (2021). https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

Reding, V. (2016). *Digital Sovereignty: Europe at a Crossroads*. EIB Institute. https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf

Regulation 1025/2012 of 25 October 2012 on European standardisation (2012. (n.d.). *Official Journal of the European Union L*, *316*(12). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1025&from=EN

RIPE NCC Engagement with External Organisations. (2020, September 18). RIPE Network Coordination Centre. https://www.ripe.net/about-us/what-we-do/engagement-external-organisations

Schmitt, F., & Debes, F. (2020). StopCovid: Cédric O demande à Apple de « lever les barrières techniques ». *Les Echos*. https://www.lesechos.fr/tech-medias/hightech/stopcovid-cedric-o-demand

e-a-apple-de-lever-les-barrieres-techniques-1196550.

Sion, L., Landuyt, D. V., & Joosen, W. (2020). The Never-Ending Story: On the Need for Continuous Privacy Impact Assessment. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 314–317. https://doi.org/10.1109/EuroSPW51379.2020.00049

Sydell, L. (2016). *In Fighting FBI, Apple Says Free Speech Rights Mean No Forced Coding*. National Public Radio. https://www.npr.org/sections/alltechconsidered/2016/02/27/468308775/in-fighting-fbi-apple-says-free-speech-rights-mean-no-forced-coding?t=1603297458110.

Tan, Z. A. (2001). *Comparison of Wireless Standards-Setting—United States Versus Europe*.

Taylor, E. (2019). The politics of networks: How great power rivalries infected 5G. *The Hill*. https://thehill.com/opinion/cybersecurity/441098-the-politics-of-networks-how-great-power-rivalries-infected-5g

ten Oever, N. (2020). *Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure* [Ph.D thesis, University of Amsterdam]. https://hdl.handle.net/11245.1/9dff56cd-0ec6-40fa-b136-105bed8ac243

ten Oever, N., & Cath, C. (2017). *Research into Human Rights Protocol Considerations* (Request for Comments No. 8280). Internet Engineering Task Force. https://datatracker.ietf.org/doc/rfc8280/

U.K. Competition Markets Authority. (2020). Appendix G: the role of tracking in digital advertising. In *Report on online platforms and digital advertising market study*. https://assets.publishing.service.gov.uk/media/5efb1d6ae90e075c53dfce67/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential.pdf

Universal declaration of human rights, Pub. L. No. 302 2 (1948).

Convention on the Rights of Persons with Disabilities, Pub. L. No. Resolution No. A/RES/61/106 (2006).

U.S. Department of Justice. (2020). *International Statement: End-To-End Encryption and Public Safety*. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

van Kesteren, A., & Stachowiak, M. (2007). *HTML design principles* [Working Draft]. W3C. https://www.w3.org/TR/html-design-principles/#priority-of-constituencies

van Oudheusden, M. (2014). Where are the politics in responsible innovation? European governance, technology assessments, and beyond. *Journal of Responsible Innovation*, *1*(1), 67-86,. https://doi.org/10.1080/23299460.2014.882097

Villareal, A. B. (2018). *International Standardization and the Agreement on Technical Barriers to Trade*. Cambridge University press. https://doi.org/10.1017/9781108591348

W3C Privacy Interest Group. (n.d.).

W3C Tracking Protection Working Group Charter. (n.d.).

W3C Web Application Security Group. (n.d.).

W.A.I. Interest Group. (n.d.). W3C Web Accessibility Initiative. https://www.w3.org/WAI/about/groups/waiig/

Werle, R., & Iversen, E. J. (2006). Promoting legitimacy in technical standardization. *Science, Technology & Innovation Studies*, *2*(1), 19-39,. https://doi.org/10.17877/DE290R-12756

Wilson, N. (2020). China Standards 2035 and the Plan for World Domination—Don't Believe China's Hype [Blog post]. *Council on Foreign Relations, Net Politics*. https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype

Wolfrum, R., Stoll, P. T., & Seibert-Fohr, A. (Eds.). (2007). *WTO-technical barriers and SPS measures*. Cambridge University Press. http://dx.doi.org/10.2307/20456713

Yamany. (2019). *Understanding 5G: A Practical Guide to Deploying and Operating 5G Networks*. Viavi Solutions.

Zetter, K. (2016, February 16). Magistrate Orders Apple to Help FBI Hack San Bernardino Shooter's Phone. *Wired*. https://www.wired.com/2016/02/magistrate-orders-apple-to-help-fbi-hack-phone-of-san-bernardino-shooter/

[Declaration of novelty and no competing interests]

By submitting this manuscript I declare that this manuscript and its essential content has not been published elsewhere or that it is considered for publication in another outlet.

No competing interests exist that have influenced or can be perceived to have influenced the text.

Published by

in cooperation with