Rossi, Julien; Keller, Jonathan

Article

Are internet standard developing organisations data controllers under the GDPR?

Internet Policy Review

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

Suggested Citation: Rossi, Julien; Keller, Jonathan (2025) : Are internet standard developing organisations data controllers under the GDPR?, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 14, Iss. 3, pp. 1-23, https://doi.org/10.14763/2025.3.2034

This Version is available at:
https://hdl.handle.net/10419/330354

INTERNET POLICY REVIEW

Volume 14 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Are internet standard developing organisations data controllers under the GDPR?

Julien Rossi *Université Paris 8*
Jonathan Keller *CNRS*

DOI: https://doi.org/10.14763/2025.3.2034

Published: 15 September 2025
Received: 5 February 2025 **Accepted:** 20 May 2025

Funding: The authors did not receive any funding for this research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Rossi, J., & Keller, J. (2025). Are internet standard developing organisations data controllers under the GDPR? *Internet Policy Review*, *14*(3). https://doi.org/10.14763/2025.3.2034

Keywords: Data protection, GDPR, Data controller, Technical standardisation, EU law

Abstract: In 2022, the Belgian Data Protection Authority (DPA) issued a fine against IAB Europe. It held this industry association for online advertising liable for multiple violations of the General Data Protection Regulation (GDPR) in relation to the Transparency and Control Framework (TCF). This technical standard is used by most Consent Management Platforms (CMPs) deployed on websites available from Europe. It generates a machine-readable expression of user preferences with regards to online privacy, transmitting to all stakeholders' servers taking part in the display of online advertisements. This is meant to ensure that no identifiers are stored on user devices, thus no personal data are processed, prior to any user consent. The Belgian DPA's qualification of IAB Europe as a joint controller in the operation of this standard, which has been confirmed in January 2024 by the European Union's Court of Justice, could be a significant development generating major implications for the whole internet governance ecosystem, object of the examination conducted in this contribution. However, the specifics of this case mean that it can hardly apply to all internet standard developing organisation

Introduction

In February 2022, the Belgian Data Protection Authority (Belgian DPA) issued a decision gathering an injunction and a fine against IAB Europe, an industry association for online advertisers, due to multiple violations of[1]the General Data Protection Regulation (GDPR) for the deployment of the oft criticised Transparency and Control Framework (TCF) (Matte, Bielova, et al., 2020; Morel et al., 2023). This standard adds information on user privacy preferences in messages sent between servers delivering advertisements using the OpenRTB protocol known as "one of the most widely used protocols for Real Time Bidding, which is an instant and automated online auction system of user profiles for the purpose of selling and purchasing advertising space on the internet" (ECJ, IAB Europe, 2024, §22). The TCF aims at ensuring the compliance of the real-time bidding ecosystem[2]with the EU data protection law. The Belgian DPA's investigation noted that the "TCF constitutes a separate set of policies, technical specifications, […], created, managed and administered by IAB Europe […] capable of informing users of the legitimate interests pursued by advertisers, as well as obtaining the valid consent of those users with regard to the processing of their personal data in a real-time bidding system" (Belgian DPA 2022, §37).

The TCF is implemented by most Consent Management Platforms (CMPs), deployed on a growing number of European websites to produce cookie banners. It allows them to generate a machine-readable expression of user preferences. Those banners transmit a signal (the "Transparency and Control String" or "TC String") to third-party servers participating in the online advertisement to guarantee that no identifiers are stored on user devices and no personal data are processed prior to the user's consent. Personal data processing operations in online behavioural advertising involved many joint controllers in the operation, including CMPs themselves (Santos et al., 2021). This is nothing new.

However, the qualification of IAB Europe – editor of the TCF – as a joint controller by the Belgian DPA (2022), then by the ECJ (IAB Europe, 2024), and finally the Court of Appeal of the Market Court section of the Brussels Court of Appeal (2025),

1. Even if directive 2002/58/EC (ePrivacy Directive) is mentioned by both the DPA and by the European Union's Court of Justice, both decisions are quoting it as contextual elements and not as a ground to sanction IAB Europe.
2. Defined by Michael Veale and Frederik Zuiderveen Borgesius (Veale & Borgesius, 2022, p. 227) as "a system where pre-determined advertising space, such as a banner advert on a website, or a splash screen in an app, is allocated through an auction process carried out for each requested impression".

represents a significant shift generating major implications for Standard Developing Organisations (SDOs) in EU law and potentially also in the field of internet governance. SDOs are defined as "the administration and design of the technologies that keep the Internet operational and the enactment of policy around these technologies." (DeNardis, 2020, p. 3). In this article, we apply the legal principles drawn from this case to a selection of four internet standards: the Internet Protocol, WHOIS, the Geolocation API and Do Not Track.

For the record, Article 4(7) GDPR defines a data controller as "the natural or legal person (…) which, alone or jointly with others, determines the purposes and means of the processing of personal data". The IAB TCF case raises questions on the notion of the "determination" of the purposes and means, cornerstone of the qualification of controller as stated by Article 4(7) of the GDPR, particularly in the context of standard-setting. *Prima facie*, this case appears to be a *stare decisis*, in accordance with both European Data Protection Board's (EDPB, 2021) guidelines on the concept of controllers and with ECJ's previous case law.[3]The expected impact of this decision was so light, that Advocate General Tamara Ćapeta did not even provide written conclusions.

Yet, in the realm of standard setting, particularly in the field of internet governance, standard-setters and implementers are usually distinct (Rossi, 2021). Usually, only implementers – not SDOs – are liable under the GDPR for their choices of standards and their implementation. Historically, internet standard-setting bodies were built on the notion that they would "reject: kings, presidents and voting" in favour of "rough consensus and running code" (Clark, 1992, quoted by: Russell, 2006), keeping state actors (and their laws) at bay. People taking part in standardisation work have tended to avoid discussing laws, perceived as a threat to the ideal of openness and interoperability of the internet (Cath, 2021; ten Oever, 2020) and as an obstacle to building the consensus required for the broad adoption of internet standards, the vast majority of which are not subject to any legal mandate (Rossi, 2022).

What constitutes a "standard" in internet governance parlance might differ slightly from how the term is usually used in the context of EU law, which usually speaks of "harmonised standards" in the frame of the so-called New Legislative Framework (Perarnaud & Rossi, 2023). Article 2 (1) of Regulation 1025/2012 on European Standardisation distinguishes standards adopted by international standardis-

3. We are referring to Google Spain, 2014, Wirtschaftsakademie, 2018, Jehovan Todistajat, 2018, FashionID, 2019, Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (NVSC), 2023.

ation bodies (ISO, IEC or the ITU[4]), European ones (CEN-CENELEC and ETSI), national ones, or "harmonised standards" adopted on a mandate issued by the European Commission. It thus incorporates private standards into the EU legal order, whereas internet technical standards are usually produced through much more informal processes (Hawkins, 1999) within bodies such as the Internet Engineering Task Force (IETF). Some protocols even become *de facto* standards even without any form of coordination, just by virtue of their wide adoption (Ermoshina & Musiani, 2019).

The *IAB TCF* decisions, recognising the editor of a standard as a joint controller together with its implementers, could have had significant consequences for internet governance in general, if it were to apply to bodies such as the IETF or the World Wide Web Consortium (W3C). Yet, whether SDOs are (joint) controllers or not does not necessarily restrict DPAs in their ability to ensure effective and complete protection of data subjects.

Given the specificities of the *IAB TCF* case, it is worth looking closely at the European case law on the notion of joint controllership (I.a.), before outlining the criteria used in the two decisions (I.b.). After applying these criteria to a selection of internet standards (II.a.), we will examine possibilities to ensure such effective and complete protection by using mechanisms that do not rely on qualifying standard setters as (joint) controllers (II.b). Indeed, although the Belgian DPA's decision constitutes a shift in the relationship between EU law and internet standards, its effects are limited on internet standard setting as a whole. DPAs and courts may use other strategies to ensure effective and complete protection with regards to internet standards.

How IAB Europe became a joint controller

I. a. The evolution of the concept of (joint-)controllership

The notion of "data controller" is almost as old as data protection law. Article 2(d) of the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) defined "con-

4. International Organisation for Standardisation (ISO), International Electrotechnical Commission (IEC) or the International Telecommunication Unions (ITU).

trollers of the file" as any "natural or legal person, […] who is competent […] to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them". Directive 95/46/EC introduced this notion in Community Law, defining a "data controller" as the "natural or legal person" which "alone or jointly with others determines the purposes and means of the processing of personal data".

This definition added three important conditions:

1. It added the idea that data controllers control the purposes but also the means of personal data processing;
2. It recognised the situations where multiple entities jointly determine said means and purposes;
3. It replaced "is competent" with "determines".

The Article 29 Working Party (Art. 29 WP), which has since replaced by the European Data Protection Board and brings together the EU's national DPAs, analysed this evolution as follows:

> "[…] even if the capacity to "determine" may arise from a specific attribution made by law, it would usually stem from an analysis of the factual elements or circumstances of the case: one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions "why is this processing taking place? Who initiated it?" (Art. 29 WP, 2010, p. 8)

Directive 95/46 also added a new notion: that of "data processors", natural or legal persons who process personal data on behalf of the controller. In 2014, the ECJ recognised Google as a data controller for the operation of its search engine, irrespective of whether or not it had actual control over the original data it indexes, because it defined the means and purposes of the indexation process (ECJ, Google Spain, 2014, §41). The GDPR generally takes the same approach as the Directive it replaced. It only added a specific contractual obligation for joint controllers and processors but this formality is not essential, since DPAs and courts can requalify them on factual observations. This is underlined by EDPB Guidelines 1/2019 stating that "the concept of controller is a functional concept, it is therefore based on a factual rather than a formal analysis" (EDPB 2019, § 21), and that "it is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way where the factual circumstances say something else" (EDPB 2019, §28). This appreciation of the reality is useful for complex

and networked IT environments (Mahieu et al., 2019).

The ECJ's case law has interpreted data protection law with a view at guaranteeing "effective and complete protection" (ECJ, FashionID, 2019, §50) by favouring a broad interpretation of the concept of joint controllership. In both *Wirtschaftsakademie* (in 2018) and *FashionID* (in 2019), using Facebook to create a "fan page" or a like button on a website was deemed an act of joint definition of the purposes and means by which this social media platform would process personal data, even if none were stored, accessed or processed by the company creating the fan page or the website. Indeed, "the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page." (ECJ, Wirtschaftsakademie, 2018, §39). In *FashionID*, the Court "held that a natural or legal person *who exerts influence*[5] over the processing of personal data, *for his own purposes*[6] , and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller" (ECJ, FashionID, 2019, §68). However, it introduced a phased approach to liability under the GDPR (Mahieu & van Hoboken, 2019), adding that such liability is "limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means" (ECJ, FashionID, 2019, art. 2). In both cases, the purposes, defined as the "anticipated outcome that is intended or that guides your planned actions" (EDPB, 2021 §33), was different for each actor.

This process has shifted the legal definition of the data controller to a dynamic autonomous notion, i.e. a notion developed and solely interpreted by the ECJ, free from any influence of national laws. The *IAB TCF* case illustrates this point. The European judges left the final decision on whether or not the defendant exerts influence over the use of the TCF "for its own purposes" to the referring national court, adding nonetheless that this "view may be taken" (ECJ, IAB Europe, 2024, §64). This was later confirmed, with regard to processing operations based on the TCF, by the Brussels Court of Appeal in May 2025 (Brussels Appeal Court, Market Section, IAB Europe, 2025).

5. Emphasis added by the authors.

6. Emphasis added by the authors.

I. b. The IAB TCF case and the matter of determination in standardisation

(Joint) data controllers (jointly) determine the means and purposes of personal data processing operations. What does "determining" entail? Is there a threshold to the level of control required to be qualified as a data controller?

The EDPB's 07/2020 guidelines (published in 2021) describe two ways for a controller to "determine means and purposes". The first one, irrelevant to our study, is the determination by law. The second one is control stemming from factual influence either grounded on contractual stipulation or circumstantial elements, such as a "existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller" (EDPB, 2021, p. 11). It requires a factual examination to appreciate the "decisive influence (exerted by an entity) on the purposes and means of the processing is the controller" (EDPB, 2021, p. 13). For example, the guidelines qualify cloud service suppliers as (joint) data controllers when they contractually and unilaterally bind their clients without any negotiation margin (EDPB, 2021, p. 13).

In the 2018 *Jehovan Todistajat* case, the ECJ ruled that "a religious community is a controller, jointly with its members who engage in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching *organised, coordinated*[7] and *encouraged*[8] by that community" (ECJ, Jehovan Todistajat, Art. 3). In the *NVSC* case (in 2023), the European judges ruled that the Lithuanian National Public Health Centre was a joint controller because it had "*exerted influence, for its own purposes*[9] , over the determination of the purposes and means of the processing in question" (ECJ, NVSC, 2023, §31), despite the fact that it had not even yet entered into any contractual agreement with the company that developed the application at hand in the case.

Standard authors provide instructions on how software must be developed, without necessarily certifying compliance with these instructions, nor having access to data processed by users of its implementations. They may even lose control over the purposes for which its standards are implemented, as has been deplored by David Kristol, co-author of the IETF's specifications on the infamous HTTP cookies (Kristol, 2001).

7. Emphasis added by the authors.
8. Emphasis added by the authors.
9. Emphasis added by the authors.

The Belgian DPA's decision distinguishes between the TCF and OpenRTB, noting that "with regard to [the latter], IAB Tech Lab, which developed this open technical standard […] merely acts as a provider of the system with respect to participating organisations and therefore cannot be considered a data controller. In contrast to the TCF, the OpenRTB allows the processing of personal data in accordance with means and purposes entirely determined by the participating organisations […]." (Belgian DPA, IAB Europe, 2022, §46) The TCF differs from OpenRTB (and from other standards) in many ways. It defines a strict set of purposes, such as – in version 1.1, the version at hand in this case – "information storage and access", "personalisation" or "ad selection, delivery and reporting" (Matte, Santos, et al., 2020). Crucially for the Belgian DPA, IAB Europe requires participants to sign a contract, to pay a fee, and there are enforcement mechanisms put in place by the IAB in case the TCF policy accompanying the actual specifications are infringed (Belgian DPA, IAB Europe, 2022, §565). The payment of subscription fees and the existence of a contractual relationship granting auditing and control rights to IAB Europe weigh in favour of the ECJ's appreciation of joint controllership for the initial collection of personal data whereas the secondary uses are under the sole liability of the TCF implementers. IAB Europe even takes part in the implementation process itself: the Belgian DPA notes that it runs the *consensu.org* server, which is instrumental in the functioning of the system supported by the standard (Belgian DPA, IAB Europe, 2022, §43).

Whereas the Belgian DPA's decision provides a clear distinction between a *pure* standard-setter (IAB Tech Lab in relation to OpenRTB) and a standard-setter that *determines* (jointly with implementers) the means and purposes of the processing operations based on the specifications, which is reinforced by the Brussels Court of Appeal's (IAB Europe, 2025) ruling, the European Court tends to be less clear in parts of its decision. The qualification of IAB Europe as a joint controllers are deduced from the circumstances – which the referring court must still verify – where "the TCF established by IAB Europe contains technical specifications relating to the processing of the TC String [and] those specifications describe precisely how CMPs are required to collect users' preferences relating to the processing of personal data concerning those users and how such preferences must be processed in order to generate a TC String" (ECJ, IAB Europe, 2024, §66). Yet, this is exactly what all standard-setters do.

The ECJ's decision must, however, be read in light of the fact that the referring court described the TCF, in the questions it submitted for preliminary ruling, as a "binding technical framework". To what extent are voluntary standards "binding"?

Is the IAB TCF "binding" only insofar as those who implement it enter into an agreement with IAB Europe? Since the Court describes the TCF in the decision's final provisions as a "binding technical standard", the adjective "binding" appears to have its importance in demonstrating whether or not IAB Europe *determines* the means and purposes of processing. As such, a certain level of effective control over the implementation, or even a degree of participation in it, seems to be essential to qualify IAB Europe as a joint controller.

II. Applying the criteria from the IAB Europe decision to internet standards-setting

II. a. Case studies

In this section, four different internet standards will be examined, to determine if internet SDOs are to be considered as (joint) data controllers following the ECJ's reasoning in the IAB Europe case. They were selected with two aims in mind. First, we needed to keep our selection small, in order to conduct an in-depth analysis and be able to report on the arguments underpinning our findings. Secondly, our selection had to reflect some of the diversity that exists in the realm of internet standard-setting: some specifications are widely implemented, others are not; there are different SDOs; and they may concern different layers.

1. The Internet Protocol (IP), which "provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses" (Cerf, 1981), operates at the network layer and defines how an IP address is formed and how large packets can be fragmented into smaller packets on a computer network. Its version 4[10]is still the most widely used, despite having been updated by the IETF.
2. The WHOIS Protocol operates at the application layer, and is used to query servers providing information on registered domain names. Originally standardised by RFC 812 (Harrenstien & White, 1982), it was last updated by the IETF in September 2004 with RFC 3912 (Daigle, 2004).

10. In 2022, RIPE Labs, the research division of RIPE-NCC, an Amsterdam-based association acting as the Regional Internet Registry for Europe, the Middle East and Central Asia, estimated that depending on the method used for trafic measurement, only between 30 % and 40 % of end-users were capable of using the latest version of the IP, version 6. In June 2022, only 4.3 % of all trafic routed through the AMS-IX Exchange Point was compliant with IPv6, the rest being handled in version 4. See: Wilhelm 2022.

3. The Geolocation Recommendation, last updated, at the time of writing, in 2024 (Cáceres & Grant, 2024) enables web servers to query the geolocation data from a user device, through its "user agent" (usually a web browser, or any other type of web application). It is published by the W3C, and also operates at the application layer. It is widely implemented.
4. The W3C's Do Not Track standard, made up of two separate documents called Tracking Preference Expression (hereinafter: TPE) (Fielding & Singer, 2019) and Tracking Compliance and Scope (TCS) (Doty, 2019), which was intended to provide a possibility for web users to express privacy preferences in the context of online tracking (Kamara & Kosta, 2016), similarly, up to a point, to the TCF. It has largely been abandoned (Rossi, 2021).

We will assume that all these standards fall under the scope of the GDPR by its article 3, including its territorial scope, because they are implemented in the context of products and services offered in the EU, except maybe for some WHOIS database operators located outside of the EU and not offering their services to the EU. For each standard, we will examine whether they concern the processing of personal data, which data controllers usually use them, whether their respective SDO determines the means of processing and the purposes, whether the latter are the SDO's own purposes or not, and finally, discuss how much actual control the said SDO has over the actual implementation of the standard at hand. Although the ECJ has not extensively discussed the level of control exercised by the IAB Europe over the implementation of the TCF, it is indeed unusual for an SDO in the field of internet governance to be able to sanction implementers that do not abide by all the elements of a standard. This sets it apart from usual internet standards.

Internet Protocol

The most commonly deployed version of the Internet Protocol was originally specified in a document edited by Vinton Cerf in 1981: RFC 791. In a nutshell, it describes how each device on the internet can get a unique IP address. When a device sends out data over the network, they are divided into packets containing a header (with an origin and destination address) and a payload (the actual data being transmitted). Different kinds of IP addresses exist: some, as defined under RFC 1918 (Rekhter et al., 1996), are private, and can only be accessed within a Local Area Network, Others are public and can be accessed by any device on the internet. Internet Service Providers (ISPs) provide their customers with a dedicated fixed IP address or a dynamic one. In either case, these "addresses are protected personal data because they allow those users to be precisely identified" (ECJ, Scarlet v. SABAM, 2011, §51). Even dynamic IP addresses can be personal data to any-

one with "the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person" (ECJ, Patrick Breyer v. Germany, 2016, Art. 1).

The IP standard therefore supports the processing of personal data by its implementers, including all kinds of public and private persons running internet applications, and all of the intermediaries (ISPs, cache providers, hosting services, online platforms…) It defines means by which data linked to IP addresses (thus, personal data) are formed over the network. The RFC 791 states that it aims at providing connection, in line with the IETF's mission statement, "to make the Internet work better" (Alvestrand, 2004). This is done in a context that emphasises openness and interoperability as key values (Cath, 2021; ten Oever, 2020). The very existence of the IP standard is in line with the IETF's own purposes; yet its users use it for a wide variety of other purposes on which the IETF has no control over. In the words of the ECJ in *Jehovan todistajat*, although there can be no doubt that the IETF "coordinates" and "encourages" the adoption of the Internet Protocol, it does not "organise" it. No contractual relationship is established between the IETF Administration LLC and IP users and implementers. The fact that, despite dating all the way back to 1995 (Deering & Hinden, 1995), IPv6 is still not the mainstream version of the IP standard underlines this SDO's inability to impose its standards. It would nonetheless also be wrong to say that it does not "exert influence",[11] over how the IP is used for (partly) its own purpose: coordinating the continued interoperability of the internet.

WHOIS Protocol

The WHOIS database – which is currently being phased out in favour of Registration Data Directory Services and the Registration Data Access Protocol (ICANN 2025) – allows users to retrieve information on the owners of a registered domain name. The language used to form queries used to be specified by the RFC 812 (Harrenstein & White, 1982) before being replaced by RFC 3912 (Daigle, 2004).

Because domain name owners include private persons, operators of WHOIS databases are data controllers under the GDPR, except for cases that are out of its scope *ratione loci*. RFC 3912, however, only contains a very broad description of the how the WHOIS database works. It does not say what should or should not be in it. It is the Internet Corporation for Assigned Names and Numbers (ICANN) that actually holds the most power. This Californian non-profit is in charge of the Domain

11. As phrased in §68 of ECJ's *Jehovan todistajat*.

Name System (DNS). It also controls key resources, such as the allocation of blocks of IP addresses. Domain name registrars ultimately have a contractual relationship with the ICANN (Belli, 2016), through which it can impose certain obligations, such as the maintenance of a WHOIS database of their customers.

Arguably, the WHOIS database is not necessary as such to achieve the IETF's stated aims of interoperability and openness. Furthermore, RFC 3912 states that it only intends to describe the WHOIS protocol as is, leaving any decisions on potential changes tackling documented shortcomings to others. It is hard to support that the IETF determines the means of how personal data is processed in the WHOIS database data, and it is up to debate whether or not the purposes for which the latter operates are its own, and not those of the ICANN and other participants in the DNS. This situation was recognised by the Article 29 Working Party when it asked the ICANN – but not the IETF, which, at the time, had no legal personality – to ensure the compliance of the WHOIS database with Directive 95/46 (Art. 29 WP, 2003).

W3C Geolocation

The Geolocation Recommendation,[12] originally called the Geolocation API, was developed by the W3C to allow web servers to query the location of a user. The privacy issues identified during the development of this standard sparked renewed interest in privacy-related issues within the W3C, culminating with the creation of the Privacy Interest Group to review privacy issues in new web standards (Doty, 2020; Doty et al., 2010).

A location retrieved from a device through this API can be linked to the device's user using a combination of the device's IP address and other techniques, including web fingerprinting, which exploits various other pieces of data about a device to cross-identify a unique web user as he or she browses from site to site (Doty, 2015). Even patterns of travel linking together multiple location data points can be uniquely identifying (Radaelli et al., 2015). These issues are acknowledged within the standard, which "Privacy considerations" section recommends that user agents (like browsers) collect user consent before sharing location data.

Such data can serve the purposes of many different controllers: application vendors can use them to provide services that are based on geolocation, customise

12. The latest version can be found here: https://www.w3.org/TR/geolocation/. The latest version as of the time of writing is archived under this permanent URL: https://www.w3.org/TR/2024/REC-geolocation-20240916/.

advertisements or conduct surveillance. The W3C provides these data controllers with a standard allowing them to query location information from devices in a standardised way, thereby defining (at least in part) the means of this data processing.

Unlike in IAB Europe's cae, where both the ECJ and the Belgian DPA point out that the IAB's mission is to support the data collection practices of its members, it is not evident that the W3C initiated the writing of the Geolocation API for its own purposes. On the other hand, the specification document was written by a working group in which some participants work for implementers of the standards. The editors – those who do the actual writing of the specification – Marcos Cáceres and Reilly Grant were working, respectively, for Apple and Google, at the time they wrote the specifications. Therefore, in practice, W3C members taking part in the editing of the Geolocation standard can be assumed to have written into it the technical elements needed to support their purposes.

Finally, the W3C does not really control who implements its standards. Though it provides tools called "validators" helping implementers check the implementation of some of its specifications, this does not amount to a certification. Finally, the W3C does not have the same position as ICANN with regards to non-compliant registrars, or as IAB Europe, which determines who can participate in the OpenRTB ecosystem.

Given that "the existence of [a contractual] arrangement constitutes not a precondition for two or more entities to be classified as joint controllers" (ECJ, NVSC, 2023, §45), the mere fact that the W3C deemed it in line with its mission and interests to provide a host to work aimed at facilitating the purposes for which the Geolocation standard was written led to it having some degree of influence over not only the means (there, the influence is obvious), but also over the purposes of processing operations using the standard. However, it should be pointed out that in the *NVSC* case, the claimant had exerted direct influence over the development of a COVID-tracking application despite the absence of a formal contract with the developing company. This is a much higher level of influence than that of the W3C over the purposes for which its standard is used.

W3C Do Not Track

Do Not Track (DNT) was an initiative supported by the W3C, which chartered in 2011 a Tracking Protection Working Group aiming at delivering a way for web users to express their preferences with regards to online tracking through their

user agent (usually, this designates their browser). It was supposed to do so by adding this information to the HyperText Transfer Protocol (HTTP) headers sent to retrieve resources (such as a webpage) from a web server. Servers receiving an active DNT signal from a user were supposed to refrain from tracking (Kamara & Kosta, 2016; Soghoian, 2011). Although this initiative ultimately ended in failure (Rossi, 2021), it was an attempt to do what the TCF does: standardise user expressions of preferences towards online tracking and privacy in the context of web technology.

Although the information contained in a DNT header does not contain personal data, it is meant to be encapsulated into a data packet that contains an IP address. Furthermore, applying the rationale from *Pankki* case, the ECJ (2023), in the *IAB Europe* case, ruled that "even if a TC String did not itself contain factors allowing the data subject to be identified directly, it would still be the case […] that it contained the individual preferences of a specific user regarding his or her consent to the processing of personal data concerning him or her" (ECJ, IAB Europe, 2024, §43). Finally, given that the purpose of the DNT standard was to allow (or disallow) the tracking of individual users, and thereby provide consent for certain personal data processing operations, it would necessarily have to be linked to a targeted individual, "singled out" (pursuant to Recital 26 of the GDPR[13]) from the mass of Web users.

This is a much narrower purpose than the Geolocation standard. The W3C's Tracking Protection Working Group can thus be said to have exerted influence over the purpose from which its DNT standard would be used. The W3C arguably made these aims its own by chartering the working group. Because it set out, in two documents (TPE and TCS), the precise manner in which DNT were to be implemented, it also exercised influence over the means of processing.

However, the W3C does not have the level of control ICANN has over the WHOIS database, or IAB Europe has over implementers of the TCF. Its situation would thus *de facto* have been quite different, although this may ultimately not mean that it could not have been considered a joint controller, having indeed had influence over the purposes and means for which and in which its Do Not Track standard would have been implemented.

13. On this topic, see: Zuiderveen Borgesius 2016.

II. b. (Internet) standards and EU (personal data) law: an alternative to joint-controllership for complete and effective protection?

From the examples above and the analysis of the relevant case law, internet SDOs, in general, cannot be qualified as (joint) controllers under the GDPR, unless in hypothetical cases where they achieve the kind of control IAB Europe has over the implementation and management of the TCF. This should not impair the ability of DPAs and courts to provide complete and effective protection, and force SDOs to take data protection law into account when designing new technical specifications.

Since the New Legislative Approach (European Commission, 1985), standards play an important role within the EU legislative process. When directives or regulations are targeting an industrial sector, the EU's legislator often delegates the practical aspects to standards instead of trying to frame it. Although this is not the approach chosen by the GDPR, the AI Act, for example, relies heavily on harmonised standards. The paralegal strength of national standards could constitute a hindrance for international (based on the Agreement on Technical Barriers to Trade, 1995) and European trade (ECJ, 1979, Rewe Zentral AG v. Bundesmonopolverwaltung für Branntwein). Indeed, such norms, even when issued by private actors, may represent a strategic value for states and corporations, by setting up barriers that are in their best interests, explaining their investment in their negotiation. However, despite the growing rhetoric on digital sovereignty coming from the European Commission since 2019, actual influence of the EU over internet standard-setting remains quite limited (Perarnaud & Rossi, 2023). Internet standards may be recognised by the European Multi-Stakeholder Platform on ICT Standardisation for public procurements. Further, some standards developed by the IETF or the W3C are recognised by European standards developed by ETSI or CEN-CENELEC. For instance, web accessibility guidelines developed by the W3C are recognised by ETSI's EN 301 549 standard, which in turn implements the 2016/2102 Web Accessibility Directive. As such, standards edited by an international SDO either imply a transposition by an EU SDO or a direct effect through an explicit reference by EU secondary law. In both cases, they are directly part of EU law, as the ECJ has recognised that even harmonised standards developed based on an EU Commission mandate are part of the Union's legal order (ECJ, James Elliott v. Irish Asphalt, 2016 & ECJ, Public.Resource.Org and Right to Know v. Commission and Others, 2024). The compliance of such harmonised standards may also be scrutinised by the EPDB and the European Data Protection Supervisor. Both are qualified to provide the Commission advice on this compliance, the latter for all harmonised standards

relevant to EU institutions, the former after a mandate issued by the Commission. For example, the Article 29 WP (2017) - the EDPB's predecessor - advised against two proposed standards developed by ETSI on systems for automatic cars due to their foreseen non-compliance with the GDPR.

Internet standards tend to stand out from this picture because they are not part of the EU's legal order. Standards such as the Internet Protocol or the HyperText Markup Language (HTML), function as a sort of code setting how computer code must be written in order for it to work (Rossi, 2022). They are therefore crucial to the continued existence of the internet as an interoperable network of networks underpinning an online public sphere. As pointed out by Laura DeNardis: "Internet works because it is based on a universal technical language" (DeNardis, 2014, p. 65). Standards specify how this language works. The internet and its protocols were a reaction to state-supported attempts by ISO to create alternative standards – within the Open Systems Interconnection project – to those of the internet.

These origins influence how internet standards are developed to this day. For instance, the IETF, founded in 1986 but incorporated only in 2018,[14] was set up to work on editing documents called Requests for Comments which describe the internet's technical standards before submitting them for approval to an Internet Architecture Board (Russell, 2006). Its discussions are structured around mailing-lists and physical conferences (originally once per year) where participants come together to discuss work in progress. Rather than formal voting mechanisms as in official SDOs, the IETF works through a consensus-based approach, and requires the demonstration of successful implementations of any proposed standard prior its adoption. The W3C, founded in 1994 to provide support for standardisation work meant to support the development of this specific application which is built on top of the internet, has adopted a broadly similar approach to the writing of its technical specifications, despite some differences such as the existence of a more formal paid membership.

Unlike harmonised standards, the use of internet standards is rarely ever mandated by law. Punishment for actors infringing on the rules set out in a standard risk exclusion from the global internet, unless their market power is so important they can set the rules themselves without fear of the consequences. The relationship between internet standards and the law fits neither into the neat boxes of Hans Kelsen's hierarchy of norms (Barraud, 2012; Kelsen, 1962 [1934]), nor into alterna-

14. See the announcement made by Glenn Deen on 22 Sept. 2018: https://mailarchive.ietf.org/arch/msg/ietf-announce/8r8NFnfTx2rlWKBavNz8zHRve-w/.

tive proposals like François Ost and Michel van de Kerchove's (2010) "network" of norms. The fact that internet standards are meant to be applied globally whereas laws are territorial means that the exercise of developing standards that are compliant with all existing – and potentially contradictory – laws cannot be easily done, as it would have meant choosing *which* set of laws to comply with in cases where conflicting laws exist. Yet standards intersect heavily with politics, including fundamental rights like freedom of expression, privacy and data protection (Cath, 2021; Doty, 2020; ten Oever, 2020). As such, choosing one standard instead of another can, in certain circumstances, have legal consequences for implementers.

With regards to the GDPR, data controllers may face sanctions if they choose to ignore standards that may be considered as state-of-the-art, as was illustrated by the Dutch DPA's (2020) decision to impose a fine on a hospital which had failed to follow specific national security standards[15]. This fine was based on Article 32 of the regulation, but other articles, including art. 25 (on Privacy by Design and by Default) and 35 (on Data Protection Impact Assessments) can also be violated by data controllers choosing to implement the wrong standard (or to implement none of the right ones).

Not all proposed internet standards are successful. Decisions by DPAs and courts that conclude that a data controller has failed to meet its obligations under the GDPR because of their choice of a standard can therefore spell its doom or success, as long as it is followed by effective enforcement. This is the case regardless of whether the authors of the said standard are (joint) controllers, or not.

In conclusion: uncertainties remain, but effective and complete protection remains possible

(Joint) controllers have to comply with the GDPR. This includes, among other things, appointed a Data Protection Officer, managing a registry of processing operations, and conducting – where necessary pursuant to article 35 of the GDPR – data protection impact assessments[16]. None of which IAB Europe had done in relation to the TCF when the Belgian DPA conducted its investigations. Complying with such obligations may not be easy for an SDO that has little control – nor

15. NEN 7510, NEN 7512 and NEN 7513.

16. See §510, 516 and 524 of the Belgian DPA's decision.

knowledge – over who implements their standards, even when these standards do describe means of processing personal data, and have been written with purposes in mind that are in line with its mission statement.

The TCF stands out from most other internet standards because the IAB Europe takes active part in its implementation. Adtech vendors and CMPs that use the TCF must register, pay an annual fee, and are bound contractually, making it – for them – a binding standard, and not a voluntary one (even if entering into the agreement is, *de jure*, just an option). It would be similar to a situation in which the IETF would be in charge both of standardising the WHOIS protocol, and of running the actual WHOIS databases, which is currently done by registries that have an agreement with the ICANN.

Of course, the ECJ reminds us in the *IAB Europe* decision that:

> "The existence of joint controllership does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed in the light of all the relevant circumstances of the particular case."[17]

This is in line with the *FashionID* decision which had introduced a phased approach to joint-controllership (Mahieu & van Hoboken, 2019). Even so, this begs the question of the limits of the notion of data controller, and of whether or not it is useful to have such a broad definition. Even though operators are responsible only for the stages of the processing operation that they control, they have to fully implement the GDPR. According to its article 26, this would imply signing joint controllership contracts with all implementers. This appears quite impossible to achieve, for example, in the case of the IP standard. All of this means that, as a general rule, internet SDOs are *not* data controllers, unless they can be shown to exert effective control over the implementation phase of their standards.

The ECJ might still find it useful to further specify to what extent a data controller becomes one when determining *its own* purposes for which personal data are processed, and whether a level of control over said purposes (whether its own, or not) is required to qualify a person as such. It would address the criticism found in the academic literature stating that there is a risk that everyone may become a da-

17. ECJ 7 March 2024, IAB Europe, case C-604/22, §58.

ta controller, thereby diluting liability and responsibility (Millard et al., 2019). This would not hinder the capacity of data protection authorities and courts to exert influence over the standardisation process, given that if a given standard does not allow compliance with the GDPR *by design*, it can easily forbid its implementation and use by all data controllers subject to the territorial scope of this regulation. Therefore, effective and complete protection of data subjects is possible, even with regards to the implementation of internet technical standards, regardless of whether or not SDOs are to be considered data controllers under the GDPR.

ACKNOWLEDGEMENT

This article was developed from a working paper written to be discussed at Privacy Law Scholars Conference 2024. We thank the people present at the conference who made valuable contributions and suggestions, especially Irene Kamara, our discussant.

Court cases and DPA decisions

Belgian Data Protection Authority (Belgian DPA). (2022). Litigation Chamber, Decision on the merits 21/2022 of 2 February 2022.

Brussels Court of Appeal, Market Court section (2025). IAB Europe v. Data Protection Authority. 14 May 2025, case 2022/AR/292.

Court of Justice of the European Union (ECJ). (1979, February 20). Rewe-Zentral AG v. Bundesmonopolverwaltung für Branntwein, case 120/78.

Court of Justice of the European Union (ECJ). (2011, November 24). Scarlet v. SABAM, case C-70/10.

Court of Justice of the European Union (ECJ). (2014, May 13), Google Spain v. AEPD, case C-131/12.

Court of Justice of the European Union (ECJ). (2016, October 19). Patrick Breyer v. Germany, case C-582/14.

Court of Justice of the European Union (ECJ). (2016, October 27). James Elliott construction limited v. Irish Asphalt ltd, case C-613/14.

Court of Justice of the European Union (ECJ). (2018, June 5), Wirtschaftsakademie, C-210/16.

Court of Justice of the European Union (ECJ). (2018, July 10). Jehovan Todistajat, case C-25/17.

Court of Justice of the European Union (ECJ). (2019, July 29). FashionID, case C-40/17.

Court of Justice of the European Union (ECJ). (2023, June 22). Pankki-S, case C-579/21.

Court of Justice of the European Union (ECJ). (2023, December 5). Nacionalinis visuomenės

sveikatos centras prie Sveikatos apsaugos ministerijos (NVSC), case C-683/21.

Court of Justice of the European Union (ECJ). (2024, March 5). Public.Resource.Org and Right to Know v Commission and Others, case C-588/21P.

Court of Justice of the European Union (ECJ). (2024, March 7). IAB Europe, case C-604/22.

Dutch Data Protection Authority (Dutch DPA). (2020, November 26). Besluit tot het opleggen van een bestuurlijke boete. Stichting OLVG.

References

Alvestrand, H. (2004). *RFC 3935. A mission statement for the IETF, IETF*.

Article 29 Working Party (Art. 29 WP). (2003). *Opinion 2/2003 on the application of the data protection principles to the Whois directory.*

Article 29 Working Party (Art. 29 WP). (2010). *Opinion 1/2010 on the concepts of 'controller' and 'processor', WP169*.

Article 29 Working Party (Art. 29 WP). (2017). *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), WP252*.

Barraud, B. (2012). *Repenser la pyramide des normes à l'ère des réseaux: Pour une conception pragmatique du droit*. Editions L'Harmattan.

Belli, L. (2016). *De la gouvernance à la régulation de l'Internet*. Berger-Levrault.

Cáceres, M., & Grant, R. (2024). *Geolocation*. W3C Recommendation.

Cath, C. (2021). The technology we choose to create: Human rights advocacy in the Internet Engineering Task Force. *Telecommunications Policy*, *45*(6), 102144. https://doi.org/10.1016/j.telpol.2021.102144

Cerf, V. (1981). *RFC 791. Internet Protocol*. IETF.

Clark, D. D. (1992, July). *A cloudy cristal ball—Visions of the future (Presentation document)*. https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf

Daigle, L. (2004). *RFC 3912. WHOIS Protocol Specification*. IETF.

Deering, S., & Hinden, R. (1995). *RFC 1883, Internet Protocol, Version 6 (IPv6) Specification*. IETF.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

DeNardis, L. (2020). Introduction: Internet governance as an object of research inquiry. In D. C. DeNardis, N. Levinson, & F. Musiani (Eds), *Researching internet governance. Methods, frameworks, futures* (pp. 1–20). https://direct.mit.edu/books/oa-edited-volume/4936/chapter/625905/Introduction-Internet-Governance-as-an-Object-of

Doty, N. (2015, November 24). *Fingerprinting guidance for web specification authors (Draft)*. W3C - Privacy Interest Group. https://www.w3.org/TR/fingerprinting-guidance/

Doty, N. (2019). *Tracking compliance and scope*. W3C Working Group Note.

Doty, N. (2020). *Enacting privacy in internet standards* [PhD dissertation, UC Berkeley, School of Information]. https://npdoty.name/writing/enacting-privacy/

Doty, N., Mulligan, D. K., & Wilde, E. (2010). *Privacy issues of the W3C Geolocation API* (No. arXiv:1003.1775). arXiv. https://doi.org/10.48550/arXiv.1003.1775

Dulong De Rosnay, M. (2007). *La mise à disposition des oeuvres et des informations sur les réseaux: Régulation juridique et régulation technique* [PhD dissertation, Paris Pantheon-Assas University]. https://theses.fr/2007PA020079

Ermoshina, K., & Musiani, F. (2019). "Standardising by running code": The Signal protocol and de facto standardisation in end-to-end encrypted messaging. *Internet Histories*, *3*(3–4), 343–363. https://doi.org/10.1080/24701475.2019.1654697

European Commission. (2019). Technical harmonization and standards: A new approach. *COM*, *85*.

European Data Protection Board. (2019). *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation*.

European Data Protection Board. (2021). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*.

Fielding, R., & Singer., D. (2019). *Tracking preference expression (DNT)*. W3C Working Group Note.

Harrenstien, K., & White, V. (1982). *RFC 812, NICNAME/WHOIS*. IETF.

Hawkins, R. (1999). The rise of consortia in the information and communication technology industries: Emerging implications for policy. *Telecommunications Policy*, *23*(2), 159–173.

Internet Corporation for Assigned Names and Numbers (ICANN). (2025, January 27). *«ICANN Update: Launching RDAP; Sunsetting WHOIS»*. ICANN. https://www.icann.org/en/announcements/details/icann-update-launching-rdap-sunsetting-whois-27-01-2025-en

Kamara, I., & Kosta, E. (2016). Do Not Track initiatives: Regaining the lost user control. *International Data Privacy Law*, *6*(4), 276–290. https://doi.org/10.1093/idpl/ipw019

Kelsen, H. (1962). *Théorie pure du droit*. Dalloz.

Kristol, D. M. (2001). HTTP cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology*, *1*(2), 151–198. https://doi.org/10.1145/502152.502153

Mahieu, R., & Hoboken, J. (2019). *Fashion-ID: Introducing a phase-oriented approach to data protection?* European Law Blog. https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1

Mahieu, R., Hoboken, J., & Ashgari, H. (2019). Responsibility for data protection in a networked world on the question of the controller, 'effective and complete protection' and its application to data access rights in Europe. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *10*(1), 84–104.

Matte, C., Bielova, N., & Santos, C. (2020). Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *2020 IEEE Symposium on Security and Privacy (SP)*, 791–809. https://doi.org/10.1109/SP40000.2020.00076

Matte, C., Santos, C., & Bielova, N. (2020). Purposes in IAB Europe's TCF: Which legal basis and how

are they used by advertisers? *APF 2020 - Annual Privacy Forum*, 1–24.

Millard, C., Kuner, C., Cate, F. H., Lynskey, O., Ni Loideain, N., & Svantesson, D. J. B. (2019). At this rate, everyone will be a [joint] controller of personal data! *International Data Privacy Law*, *9*(4), 217–219.

Morel, V., Santos, C., Fredholm, V., & Thunberg, A. (2023). Legitimate interest is the new consent—Large-scale measurement and legal compliance of IAB Europe TCF paywalls. *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*, 153–158. https://doi.org/10.1145/3603216.3624966

Oever, N. (2020). *Wired norms. Inscription, resistance, and subversion in the governance of the Internet infrastructure* [PhD thesis]. Universiteit van Amsterdam.

Ost, F., & Kerchove, M. van de. (2010). *De la pyramide au réseau?: Pour une théorie dialectique du droit*. LGDJ.

Perarnaud, C., & Rossi, J. (2024). The EU and internet standards – Beyond the spin, a strategic turn? *Journal of European Public Policy*, *31*(8), 2175–2199. https://doi.org/10.1080/13501763.2023.2251036

Radaelli, L., Montjoye, Y.-A., Singh, V. K., & Pentland, A. P. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536–539.

Rekhter, Y., Moskowitz, B., Karrenberg, D., Groot, G. J., & Lear, E. (1996). *RFC 1918. Address allocation for private internets*. IETF.

Rossi, J. (2021). What rules the internet? A study of the troubled relation between Web standards and legal instruments in the field of privacy. *Telecommunications Policy*, *45*(6), 102143. https://doi.org/10.1016/j.telpol.2021.102143

Rossi, J. (2022). Écrire le code du code: Enquête sur les controverses techno-politiques au W3C. *RESET*, *11*. https://doi.org/10.4000/reset.3514

Russell, A. L. (2006). 'Rough consensus and running code' and the internet-OSI standards war. *IEEE Annals of the History of Computing*, *28*(3), 48–61. https://doi.org/10.1109/MAHC.2006.42

Santos, C., Nouwens, M., Toth, M., Bielova, N., & Roca, V. (2021). Consent management platforms under the GDPR: Processors and/or controllers? *APF 2021 - Annual Privacy Forum*, 47–69.

Soghoian, C. (2011, January 21). *The history of the Do Not Track header*. Internet Archive. https://web.archive.org/web/20110809034906/http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html

Veale, M., & Zuiderveen Borgesius, F. (2022). Adtech and real-time bidding under European Data Protection Law. *German Law Journal*, *23*(2), 226–256. https://doi.org/10.1017/glj.2022.18

Violet, F. (2003). *Articulation entre la norme technique et la règle de droit*. Presses universitaires d'Aix-Marseille.

Wachter, S. (2024). Limitations and loopholes in the EU AI Act and ai liability directives: What this means for the European Union, the United States, and beyond. *Yale Journal of Law and Technology*, *26*(3), 671–718.

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

RESEARCH
FOR THE
DIGITAL AGE

in cooperation with

UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies