What Rules the Internet?

A Study of the Troubled Relation Between Web Standards and Legal Instruments in the Field of Privacy

---

Abstract

There is a wide variety of policy instruments that political entrepreneurs wishing to influence policy outcomes in the field of Internet Governance may choose from. There is a strategic dimension to this choice. This paper studies how standards and laws interact in the governance of Web privacy, by looking at the case of two groups within the World Wide Web Consortium (W3C): the Tracking Protection Working Group and the Privacy Interest Group. Despite the prevalence of discourses stating that the realm of Internet standards are free from the "weary giants of flesh and steel" John Perry Barlow referred to in his *Declaration of Independence of Cyberspace*, laws, or at least some of them, do exercise a significant amount of influence in the shaping of Web standards dealing with privacy. They were quoted arguments by participants trying to settle disagreements. They influenced certain – but not all – sections of the proposed Do Not Track specifications. This influence should not, however, be confused with a clear recognition that laws are, or even should be superior to standards in a hierarchy of norms that would be impossible to establish due to the nation-bounded nature of laws against the global scope of Web standards.

Introduction

As Laura DeNardis has famously pointed out: “the Internet is governed” (DeNardis, 2014, p. 222). Once that has been established, the next item on the agenda is usually to figure out *who* governs or should govern the Internet. Instead, this paper proposes to explore *what* governs the Internet, or in other words, on the various policy instruments that can be used by those who pllay a role in Internet Governance (IG).

Policy instruments are defined by Pierre Lascoumes and Patrick Le Galès as “tools […] that allow governmental action to take shape and become operational[1]” (Lascoumes & Le Galès, 2005b, p. 12). This category includes i.a. laws, taxation and distribution of wealth, but also standards (Borraz, 2005), artefacts (Lavelle, 2009; Winner, 1980), types of procedures (Dehousse, 2005), and public relation campaigns (Butler, 1997, 2010; Ollivier-Yaniv, 2018)[2]. The choice of policy instruments is, by itself, a political decision and has effects on the policy outputs that are produced. More importantly, policy instruments are technical tools that are produced and used by a variety of actors, and not only state actors (Lascoumes, 2004). This makes this concept very relevant to the study of a field such as Internet Governance in which states are just one category of actors taking part in its complex decision-making processes to shape public action.

“Code is Law” (Lessig, 1999). Code itself often complies with technical standards, such as Requests for Comments edited by the IETF (Braman 2010). Some of those standards are deliberately designed to produce policy outputs (Nick Doty & Mulligan, 2013). Joël Reidenberg’s definition of *Lex Informatica* includes both code and standards (Reidenberg, 1997). Romain Badouard, Clément Mabi and Guillaume Sire (Badouard et al., 2016) showed that some key actors produce artefacts constraining user behaviour and contributing to the production of new forms of algorithmic governmentality. Joseph Zittrain (Zittrain, 2003) showed the role played by the distribution of control over some key Internet infrastructure elements in the overall governance of the Internet, but also showed that there are attempts by the courts to enforce legal instruments upon those who are in charge these “key points of control”, like Internet Service Providers (ISP’s). Private law instruments, such as peering contracts between such ISP’s (Massit-Folléa, 2014), or patent policies by standards-setting organisations (Contreras, 2016), also produce policy effects. Finally, literature on “digital constitutionalism” (Celeste, 2018) shows that there is a push by some actors to adopt new transnational fundamental human rights principles that all other Internet governance (IG) policy instruments should comply with.

Standards, just like laws, are instruments of public policy (Borraz, 2005). They are performative speech acts (Austin, 1962; Laugier, 2004) relying on their circulation on written supports to act upon social reality (Fraenkel, 2006; Gougeon, 1995). There is, however, a great difference between laws and standards. Hard law instruments may be enforced with the use of force by public authorities, whereas soft law instruments like standards rely on consensus worded in technical terms and market adoption to gain effect. French academic literature distinguishes between a “standard” and a “norme” (see: Borraz, 2005). A “norme” is a document produced by the collaboration of different authors who agree on a consensus for technical specifications. ISO standards, RFC’s and W3C recommendations enter that category. On the other hand, a mere “standard”, like the Signal protocol (Ermoshina & Musiani, 2019), does not undergo a process of consensual negotiation and (at least

1 Translations are my own.
Original text: “outils […] qui permettent de matérialiser et d’opérationnaliser l’action gouvernementale.”

2 For a typology, see: (Lascoumes & Le Galès, 2005a, p. 361).

formally) collegial writing process, but becomes an effective standard because products that follow its specifications become *de facto* dominant on a given market. Some technical standards (in the English meaning of the word) are in between the French “normes” and “standards”. For example, the Transparency and Control Framework is a standard developed by a single industry organisation: the Interactive Advertisement Board (IAB)[3] in order to specify ways in which consent to personal data collection for advertisement purposes, including tracking, is to be collected. Many Consent Management Platforms, like Didomi or Quantcast, follow this standard, which is indeed the product of a discussion, but with only one type of stakeholder within one single organisation, where the IAB was but one stakeholder among others in the Do Not Track project. In this paper, however, I shall use the English word *standard* to talk both about French “normes” and “standards”.

Legal scholarship identifies a hierarchy between legal instruments. Hans Kelsen established a “hierarchy of norms” (Kelsen, 1962 [1934]) where “lower” norms are only valid if they are compatible with a “higher” norm. Typically, laws should comply with constitutional norms. The relation between national laws and international treaties is trickier. For example, according to the European Court of Justice, European Union (EU) law always prevails above national law, even constitutions[4]. The recent decision by the German constitutional court establishing that the German Bundesbank[5] must disobey legally binding decisions by the European Central Bank has recently reminded the world that it disagreed, and will certainly lead to a lot of debate among constitutional law scholars.

Following a legal perspective, the hierarchy of norms on the Internet should ideally follow this order: (1) the Law, (2) technical standards, (3) running code, (4) compliant use cases/implementations. Yet the picture is much more complex. The Internet is a global piece of infrastructure, and there are many competing and conflicting laws pretending to govern it. Some of these laws are in conflict with human rights principles. Running code tends to come first, before it leads to standardisation, and standards often compete with one another (Ermoshina & Musiani, 2019; Sire, 2017). Some software do not comply with any standard, or not well. And this leads to a variety of both compliant and non-compliant use cases and implementations.

Several standards-setting organisations, like the IETF, were born from the desire of certain Internet architects to “secede” from the Westphalian world-order. As David Clark phrased it in a 1992 presentation, they rejected “kings, presidents and voting” in exchange for “running code and rough consensus” (Russell, 2006). How does that work in practice? Did Internet standards indeed manage to secede from “weary giants of flesh and steel” (Barlow, 1996) at least in the shaping of Internet standards? If so, “running code”, the standards they implement, infrastructure choices and private contracts should be the main legal instruments used to govern the Internet. Laws should be more or less irrelevant, or at least they should operate separately from technical decision-making happening in fora like the IETF or the W3C.

There are many areas in which technical decision-making intersects with state-driven public policy. Sometimes, the relation between standards and laws is conflictual. For instance, the (de)regulation of cryptography and its use in Internet communications has been, and still is to a large extent, a very contested matter (Tréguer, 2019). Privacy is another typical area of intersection between

3 See: https://iabeurope.eu/tcf-goverance-board/ .

4 ECJ 17 December 1970 Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, case 11-70.

5 BVerfG, Judgment of the Second Senate of 05 May 2020 - 2 BvR 859/15

the technical and the political. On the one hand, Lawrence Lessig (Lessig, 2000) argued that to a certain extent the Internet Protocol protects user privacy because an IP address does not identify the user directly. At the same time, the development of tracking technology – from cookies to fingerprinting – has allowed some actors to circumvent the non-identified nature of IP addresses. These techniques have been especially useful for the displaying of personalised advertisement by the advertising industry. One of its associations, the Interactive Advertisement Bureau, is currently actively promoting a standard called the Transparency Control Framework (TCF), which has been criticised as including elements that conflict with rules established in legal instruments such as the EU's General Data Protection Regulation (GDPR) (Matte et al., 2020). In practice, websites tend to abide by the former more than the latter (Degeling et al., 2019; Nouwens et al., 2020; Utz et al., 2019). Privacy is also a field of public action which has seen many attempts by certain norm entrepeneurs to adopt standards that would make the Internet and/or some of its applications more privacy-friendly. Such *techno-policy* standards, to use a concept borrowed from Deirdre Mulligan and Nick Doty (2013), are being discussed among others within the World Wide Web Consortium (W3C), which is where the field study presented in this paper was conducted.

Case study and methodology

The World Wide Web Consortium (W3C) is an organisation hosting discussions on standards related to the World Wide Web, such as HyperText Markup Language (HTML) and Cascading StyleSheets (CSS). It also publishes recommendations on a variety of other technologies with heavy privacy implications, such as a Geolocation API, a Web Payments API or a Media Capture and Streams recommendation for access to microphones and video cameras. The W3C has hosted groups working on privacy preserving standards ever since 1997, when it became the host of the Platform for Privacy Preferences (P3P) project. Between 2011 and 2019, its Tracking Protection Working Group (TPWG) worked on a "Do Not Track" signal that browsers would send to web servers if a user did not want to be "tracked". Since 2011, another group, the Privacy Interest Group (PING), brings together a group of experts advising other working groups on how to implement privacy by design principles into their standards.

I studied these groups during a doctoral research project on the shaping of data protection public policy. One of the aims of this research was to investigate the existence of differences between discourses on privacy and data protection in classical state-centred decision-making arenas such as the Council of Europe and the European Union, and technical standards-settings organisations like the W3C. In the end, it appeared that in both settings, discussions were dominated by common references to a liberal privacy paradigm (Bennett & Raab, 2003; Fuchs, 2011) in which privacy is defined as an individual right to informational self-determination, or as W3C participants put it, "user control" (Rossi, 2020). It also appeared that legal developments in the EU culminating in the entry into application of the GDPR in May 2018 had a much greater impact on discussions within the W3C than initially assumed, given the prevalence of a narrative portraying technical decision-making as independent or at least agnostic towards the law. This would suggest that the work of privacy advocates (Bennett, 2008) who started working on the production of new informational privacy norms in the early 1970's (Hondius, 1975) and organised themselves into a transgovernmental network of policy entrepreneurs that had a pivotal influence on the slow but steady global expansion of data protection law (Newman, 2008) also achieved some success in shaping debates, if not outcomes, in private technical standards-setting fora.

This research was conducted between 2016 and 2019 and focuses on a period between 2011 and late 2018, but also includes elements on the P3P project which took place roughly between the mid-1990's and the mid-2000's[6].

Data was compiled from different sources.

First of all, I went through documents produced by the P3P working group (P3P WG), the Tracking Protection Working Group (TPWG) and the Privacy Interest Group (PING) to compare the definitions and principles I could find with legal provisions in EU law. I looked in particular at the definition of the notion of "personal data" and/or "personnally identifiable information" to study their parallel evolution.

Taking inspiration from work conducted by Nick Doty on security and privacy considerations in RFCs (Doty 2015), I generated statistics of the use of some significant terms, such as "law", "privacy", "gdpr" and "personal data" in 53 public W3C mailing-lists, including those tied to the P3P WG, the TPWG and the PING. I developed scripts to parse over 340 000 e-mails to look for such keywords, participants, and map these out. This helped me observe when and where there were pikes in the discussion on these topics, and to track clues about how the discussion moved from one working group to another. It also helped me select a narrower set of e-mails that I could read for qualitative document analysis (Bowen, 2009), providing factual elements but also enabled me to map the evolution of discourses and positions of actors involved in this process, with regards to privacy and legal developments in the EU. I focused mainly, but not exclusively, on e-mails exchanged in the frame of a heated debate on the definition of "tracking" that took place between 2011 and 2013 within the TPWG.

I also conducted semi-structured qualitative interviews with 10 members of these groups. These interviews were centred around their perceptions on privacy and their discursive strategies, but they also yielded a lot of information on how these actors perceived the relation between their efforts and the law. Finally, I took part in the 2018 Face-to-Face meeting of the PING in Lyon, during the W3C's annual Technical Plenary and Advisory Committee (TPAC), to observe the discussions and get a better understanding of the group's functioning.

I will proceed with the presentation of discourses produced within the W3C that portray it as independent from state-centred legal developments. I will then show how participants did in fact employ arguments based on legal requirements to defend their ideas and interests, before discussing the interaction between legal instruments and Web standards in the field of privacy.

Discourses on the Role of Legal Instruments on the Ground

Standards-setting bodies such as the IETF and the W3C were created in part because of the will of its members to keep states at bay. It was believed by their founders that this would increase the quality of standards, as there would be no public authority that would be able to force the adoption of mediocre ones (Russell, 2006). Some interviewed W3C PING and TPWG participants shared the impression that they were staying "away" from legal considerations:

6 The P3P project initially started outside the W3C, but it became a W3C Working Group in 1997, with support from Tim Berners Lee and the FTC. The project was closed in 2006, with the publication of version 1.1. of the P3P specification, but it was never widely implemented.

> “I think that at least my experience with standards is that, first of all, it tends to stay reasonably far away from the law. […] It sometimes comes up, but it doesn't tend to dominate discussions.” (Interview with a member of the PING[7])

This was explained by another member by the fact that laws often differ greatly from one jurisdiction to another, whereas the W3C is making standards for something global:

> “Regulations differ so much between jurisdictions […]. The goals of W3C are to develop these things that are going to be complemented and used worldwide” (Interview with a member of the PING)

With regards to Web standards and privacy legislation, it can succesfully be argued that the W3C is *not* a data controller. Editors cannot predict the whole range of use cases of their specifications. According to Simon Rice, Technology Group Manager at the Information Commissioner's Office (the British Data Protection Authority) and member of the PING at the time of the interview:

> “[…] Protocol designers [are not] data controllers specifically. So it's difficult to say: does this protocol comply with European legislation? In a lot of cases it doesn't need to. Because it's just a protocol. It's not actual processing, there is no data controller.” (Interview with Simon Rice)

Furthermore, according to some W3C participants, legal experts are not good at writing down rules regulating the Internet, especially its technical elements. They portray legal texts as unclear to computer engineers, sometimes unhelpful, and therefore a good reason to pre-empt potentially mediocre legislative action by adopting voluntary rules set into widely accepted standards:

> “The meta point here is that we'd rather see the folks close to the technology think about the user interaction and security *now*, and document the results of that, than have a bunch of privacy commissioners design UI and pass a law about it -- we've had that with the "cookie directive" in the EU; I'd rather not see a repetition of that for location and other device APIs. » (Thomas Roessler, 12 May 2009)

> “Worst case, the law itself will serve as the compliance spec. However, it would help companies to have something translated from wonk to geek, something more easily implementable. Reference implementations and source code would help. » (Aleecia McDonald, 19 December 2016)

With one exception, guidance documents reviewed in this research[8] and produced by W3C participants on privacy do not include any reference to laws. Instead, there may be references to other documents written by Internet standard-setting bodies. For example, a document called *Privacy Considerations for Web Protocols*, edited by Hannes Tschofening and Nick Doty, and also the *Self-*

7 Only the names of interviewed participants who agreed to the publication of their name attached to the quotes are indicated.

8 Reviewed documents include: *Privacy Considerations for Web Protocols* (28 July 2020), *Self-Review Questionnaire: Security and Privacy* (17 June 2020), *Mitigating Browser Fingerprinting in Web Specifications* (26 March 2020), *Tracking Compliance and Scope* (22 January 2019), *Tracking Preference Expression (DNT)* (17 January 2019), *Specification Privacy Assessment (SPA) Creating Privacy Considerations for W3C Technical Specifications* (28 June 2013), *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification* (13 November 2006).

Review Questionnaire: Security and Privacy published jointly by PING and the Technical Architecture Group (TAG) include references to several IETF documents, including RFC 6973 on *Privacy Considerations for Internet Protocols*.

The one exception I mentioned is an unofficial draft proposed in 2013 by Nokia engineer Frank Dawson, called *Specification Privacy Assessment*, which includes references to the OECD Privacy Principles, the US Federal Trade Commission (FTC) Fair Information Practice Principles and, more importantly, to EU Directive 95/46/EC on the protection of personal data. This document, however, has no official status and, as of July 2020, was no longer listed on the homepage of the W3C PING[9]. Version 1.1 of the P3P specification, published as a Working Group note in 2006, only links to examples of legislation – including the 1995 European directive – in an appendix. This note, which presented itself as being "complementary" to existing legal requirements, was officially withdrawn by W3C in 2018 and was never widely implemented.

Therefore, looking at the history of bodies like the IETF and W3C, listening to impressions shared by W3C participants, and looking at documents produced within the W3C on the topic of privacy, it would indeed appear that standards are at least in a large part disconnected from legal requirements and maybe even the realm of legal discourse. There is no explicit hierarchy whereby W3C recommendations have to comply with the law. In other words, techno-policy standards such as P3P and Do Not Track as well as privacy considerations sections in other standards – like the Geolocation API – are there to protect the "privacy" of Web users, not (simply) to help implementers comply with legal requirements. Even if participants are aware that the standards they are working on may help them do so, this would be just a side-benefit.

Legal Instruments Used as Arguments in Techno-Policy Debates

At least in the field of Web privacy, debates on privacy nonetheless contain a lot of references to the law. Legal requirements are often used as arguments in debates. This was especially the case in the discussions on the two Do Not Track draft recommendations: *Tracking Preference Expression*, which explains how a browser should communicate the expression of user preference, and *Tracking Compliance and Scope*, which describes how a server should respond to a Do Not Track signal.

Between 2011 and 2013, a heated debate took place within the W3C TPWG on what "tracking" exactly means (Rossi, 2020, pp. 466–478). At stake was what the Do Not Track signal would mean for data flows between a first-party, the website explicitly requested by the user, and third-party web elements called by the first-party website generating data flows between the user's computer and third-party websites that he or she may not be aware of. Does a website collecting browsing data about only its first-party users qualify as "tracking", or does the latter only refer to the action of recording a user's navigation *across* websites[10]?

One participant, Ninja Marnau, a lawyer working for the DPA of Schleswig-Holstein, wrote to the group in November 2011 and argued that a standard allowing first-party sites to collect data even if the Do Not Track signal has been turned on by the user would be useless to ensure compliance with the EU's e-Privacy Directive:

---

9 This document was listed in July 2019 on the homepage of W3C PING, as can be seen using the WayBack Machine: https://web.archive.org/web/20190709014327/https://www.w3.org/Privacy/IG/

10 E-mails related to this controversy have been compiled into a single issue on a bug tracker used by the W3C TPWG, which can be found following this link: https://www.w3.org/2011/tracking-protection/track/issues/5 .

> “If you agree on not including first party tracking, you decide to not address in which way soever the requirements of Art. 5 III of the E-Privacy Directive concerning first parties. Lost opportunity.” (Ninja Marnau, 30 November 2011)

Another participant, Shane Wiley, an engineer working at Yahoo, insisted that she was wrong because he had heard other lawyers stating the opposite:

> “ The ePrivacy Directive does not require consent for “legitimate” cookie use to deliver a service and most DPAs I've spoken to have felt this covers 1st party cookie use and that only “3rd party advertising cookies” are the true target of the ePrivacy Directive.” (Shane Wiley, 30 November 2011)

While the validity of the legal analysis in this last quote is debatable[11], what is relevant here is to note the use of legal arguments is accepted as legitimate by both sides of the “tracking” debate. Given the fact of the existence of binding regulations requiring an expression of consent for the collection of personal data in situations like the collection of such data for marketing purposes, people like Rob van Eijk, who was working at the Dutch Data Protection Authority, framed the Do Not Track project as an opportunity to create a technically sound mechanism which would make compliance easier and less expensive if such legal requirements were carefully taken into account in the design of the protocol:

> “It is clear that the group is not calling for (re)creating P3P. The discussion at the moment has come to the point of explorating how to acoomodate [sic] 'hooks' in the DNT protocol/spec to enable data controllers to become compliant with the EU requirement of explicit, informed consent.” (Rob van Eijk, 28 March 2017)

When asked about his argumentative strategy to defend his proposals on privacy, Rigo Wenning, a lawyer and a W3C staff member who took part in both the P3P and the Do Not Track projects, answered: “with regulation, with European privacy regulation[12]”. According to an American engineer who was involved in the W3C PING: “I think that the GDPR is a good focal point for privacy experts. Because you can look at the GDPR and see what’s going to be happening all across the world.” And according to Mozilla engineer Sid Stamm, one of the early proponents of the Do Not Track mechanism:

> “From the beginning, the advertising industry, at least in the United States, was very keen to be at the table. […] And the reason was because the Federal Trade Commission had more or less endorsed the W3C's efforts to standardise this Do Not Track thing. And that suggested to the industry that is actually currently self-regulated for the most part: get in the room with these technologists, and decide with them what you're gonna do, or we're gonna decide for you. It was legislative pressure, you know, at its best.” (Interview with Sid Stamm)

Another stake in the debate on “tracking” was whether “not tracking” should mean an absence of data collection, or merely an opt-out on personalised advertisement. In order to ensure that it would not be the latter, John Simpson shared a letter of the Article 29 Working Party with the TPWG on 5 March 2012. In this letter, Jacob Kohnstamm, chairman of the Working Party, insisted that an “essential condition for DNT to meet the requirements of European data protection law is that a DNT-

11 On cookies, tracking and e-Privacy directive, see i.a.: Coupez & Péronne, 2020; Degeling et al., 2019; Jabłonowska & Michałowicz, 2020; Matte et al., 2020; Santos et al., 2019.

12 Original version: « Avec la régulation, avec la régulation de la vie privée européenn ».

setting in a browser means that users should no longer be tracked, instead of just not being shown targeted advertisements." (Kohnstamm 2012).

Each W3C Working Group is defined by its charter, which includes a starting date and a date when the group is expected to have concluded its assigned mission. In 2016, the TPWG petitioned the W3C's Advisory Committee for an extension of its charter. To do so, it had to prove that it was making progress, and that further progress was still relevant. In December, Baycloud co-founder Mike O'Neill shared a link to a webpage of the International Association of Privacy Professionals summarising a leaked draft of the Commission's proposal for an e-Privacy Regulation that would replace the current e-Privacy Directive:

> "This a good summary of the leaked draft ePrivacy regulation, and points out the relevance to Do Not Track:
>
> https://iapp.org/news/a/eprivacy-leaked-draft-the-good-the-bad-and-the-missing" (Mike O'Neill (1), 16 December 2016)

Jeff Jaffe, who was – and still is – CEO of the W3C, answered that he "didn't see where this pointed to any W3C Standard for Do Not Track, or any compliance regime." (Jeff Jaffe, 16 December 2016). This led to several lengthy answers, among others by Mike O'Neill (16 December 2016 (2)), Walter van Holst (16 December 2016) and Aleecia McDonald, the latter insisting that:

> "There are almost certainly other options that could work, given enough effort. They'd be starting from scratch.
> Enforcement of EU laws begins in a year and a half.
> W3C DNT started in Fall 2011. It's not so far off from meeting EU compliance. It seems worth a final push. I say that as someone who would rather dental work to more DNT discussions." (Aleecia McDonald, 16 December 2016)

On the same day, Matthias Schunter, engineer at Intel and co-chair of the TPWG, shared an e-mail sent by Jan Philipp Albrecht, the rapporteur of the GDPR in the European Parliament, to Tim Berners-Lee (Director of the W3C), Jeff Jaffe and him, in which he clearly defended an extension to the group's charter:

> "Hi Folks,
> we received very strong support from the EU (enclosed) that endorse our renewed focus on compliance with EU regulations and would welcome browser/tool-support for opt-in to data collection in the EU.
>
> Regards,
>
> matthias
>
> -------- Forwarded Message --------
>
> […]
>
> Dear friends in the W3C,

> Allow me to address you with a few remarks on the W3C Tracking Protection Working Group and its future work. […]
>
> 2. On many web sites, including those run by the major online publishers, there can be several hundred "third-party" servers accessed when a page is visited. If personal data is processed by these servers, the GDPR requires that the identity of the relevant data controller, its claimed legal basis and purpose for processing be declared. Other than described in the Do Not Track Tracking Preference Expression (TPE) document, there is currently no standardised web platform method for doing this. […]
>
> 9. For all these reasons, there is more work to do in your area of expertise. I urge you therefore to extend the mandate of the TPWG until after the end of 2016.
>
> Best regards,
>
> Jan Philipp Albrecht" (Matthias Schunter, 16 December 2016)

Thanks in part to legislative pressure and the support of actors like Jan Philipp Albrecht and the Article 29 Working Party, the TPWG was rechartered in January 2017. A table summarising the Charter history of the group shows how this had an influence on the stated goals of the group themselves:

Charter Period	Start Date	End Date	Changes
Initial Charter	2011-09-08	2012-07-31	N/A
Charter Extension		2014-04-30	none
Charter Extension		2015-12-31	none
Charter Extension		2016-12-31	none
New Charter	2017-01-26	2017-12-31	Refocused on TPE and EU compliance.
Charter Extension		2018-09-30	none

Screenshot taken on the webpage of Tracking Protection Working Group Charter[13].

In 2018, when Xueyuan Jia announced to the group that its charter was again extended, she made references to the need for further progress to make sure Do Not Track could be used to comply with EU legal obligations:

> "When we last re-chartered the Working Group […], the Director indicated a main focus for the extended implementation phase was to demonstrate the viability of DNT to address the requirements for managing cookie and tracking consent that satisfies the requirements of EU privacy legislation." (Xueyuan Jia, 10 April 2018).

In 2019, however, she made an announcement to the *public-tracking* mailing-list that the TPWG was closed, due to a lack of activity and adoption of the standard[14].

13 This page can found at: https://www.w3.org/2016/11/tracking-protection-wg.html#history
14 See the e-mail she sent on the 17th of January, 2019.

Understanding the Use of Legal Arguments in Techno-Policy Standards-Setting Processes

In order to understand this apparently paradoxical use of legal arguments in an arena that is supposed to be at arm's length from "kings, presidents and voting", one has to bear in mind that the W3C has no authority to coerce actors within the Web ecosystem to abide by its recommendations, even those that are officially endorsed. Even its authority on the HyperText Markup Language (HTML), a cornerstone of Web technology, is contested by the existence of a rival organisation set up in 2004: the Web Hypertext Application Technology Working Group (WHATWG) (Sire, 2017). This is why successful standards are those around which there is a technical consensus that it is the best working solution for the problem it solves. This in turn is why the prevailing norm of discourse ethics, observed by Luca Belli (Belli, 2016, pp. 368–370) at the Internet Governance Forum (IGF) and at the IETF is also very present at the W3C (Rossi, 2020, pp. 450–481). The launch of a debate on the definition of "tracking", sponsored by Roy Fielding, who was working for Adobe, a company involved in the ad industry, was perceived by many privacy advocates as a tactical manoeuvre to delay consensus and contribute to the failure of the project[15]. Usually, everything is done in order to preserve consensus so that a draft can proceed on the path towards being a widely implemented standard. The W3C's guidebook for participants is tellingly called the *Art of Consensus*[16].

Even though the technical object of the discussion actually often acts as a mediator for political or moral debates, participants are reluctant to openly engage in discussion on values, politics or philosophy in order to avoid delaying an already complex decision-making. This is why, for example, the authors of the draft *Privacy Considerations for Web Protocols* deemed it important to specify that:

> "This document does not attempt to define what privacy is (in a Web context). Instead privacy is the sum of what is contained in this document. While this may not be exactly what most readers would typically assume but privacy is a complicated concept with a rich history that spans many disciplines and there remains confusion over the meaning." (Tschofening and Doty, 2020)

So in this context, where consensus is paramount, where people may agree with the sentence "user privacy is a good thing", but disagree on what that means and on the extent to which it should prevail over other interests – such as the interests of web publishers and advertisers to profile their visitors – references to the law are one of the ways in which it becomes possible to defend values while presenting the argument in a technical manner, signalling that: this is not (only) about (my potentially subjective) belief and value system, but also about doing what is *technically* best in order to comply with (objective) legal requirements.

Of course, another reason is simply the fact that pressure from public authorities was an important factor in convincing industry representatives to take part in discussions on projects like P3P and Do Not Track (Nick Doty & Mulligan, 2013, p. 145; Kamara & Kosta, 2016; Kohnstamm, 2012;

15 On 10 December 2011, Jonathan Mayer wrote to the public mailing-list of the TPWG that "The working group has now swirled around the "How do we define tracking?" and "How do we define Do Not Track?" drains several times. […] This approach is not productive. […] I would propose that we mark ISSUE-5 as POSTPONED since achieving consensus on it is not necessary to the working group's tasks." (Jonathan Mayer, 2011). According to Rigo Wenning in an e-mail sent on 12 January 2012: "Roy is trying to import the difficult meaning discussions of the Compliance Specification into the DNT Specification […]" (Rigo Wenning, 2012). The debate was called a "diversion" by Rigo Wenning in an interview.

16 See: https://www.w3.org/Guide/

Soghoian, 2011; FTC, 2011, Matthias Schunter e-mail of 16 December 2016). Some of the people who participated in TPWG and/or PING, like Ninja Marnau, Simon Rice, Vincent Toubiana and Rob van Eijk were also working for Data Protection Authorities at the same time, and gave some input. In 2009, the European Union amended its 2002 e-Privacy Directive to compel websites to ask for opt-in consent to save data (such as cookies used for cross-site tracking purposes) on a user's device. Recital 66 of the amending directive[17] stated that "where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application." In 2013, California amended its Online Privacy Protection Act[18] to force websites to disclose how they respond to the Do Not Track signal. It was only a disclosure law, however, that left websites free to ignore their visitors' privacy preferences expressed through the mechanism. In 2016, the EU adopted a General Data Protection Regulation which provided for fines up to 4% of global turnover for certain categories of violations of data protection rights, including failure to collect valid consent. It contains a definition of "personal data" that is large enough to cover data able to "single out" an individual and profile her for marketing purposes even without being able to identify her by name (Zuiderveen Borgesius, 2016). In 2017, the European Commission tabled a Regulation proposal to replace its 2002 e-Privacy Directive. Its Recital 22 is even more explicit than Recital 66 of the 2009 Directive on its support to the Do Not Track project[19]. Its article 9 (3) states that "[…] where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet." Its explanatory memorandum mentions Do Not Track as a desirable standard for the expression of user consent (EU Commission COM (2017) 10 FINAL, p. 8).

Another possible explanation, though perhaps less potent than the previous one, to the presence of legal arguments on privacy within the W3C is that legal materials may be used as a source of expertise, or at least as a source of inspiration for rules and definitions. This is reflected in the *Specification Privacy Assessment* draft document that was proposed by Frank Dawson to the PING, which references an article written by Paul Schwartz and Daniel Solove on the definition of "Personally Identifiable Information" (Schwartz & Solove, 2012). It can also be seen in documents produced by the TPWG. Since 2012, successive Tracking Preference Expression draft specifications include terms such as "personal data" and "controller" which are borrowed from data protection law[20]. The W3C Security and Privacy Questionnaire includes a reference to RFC 6973, which defines "personal data" as "[a]ny information relating to an individual who can be identified, directly or indirectly", a wording that is almost exactly the same as in that found in the Council of Europe's

17 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

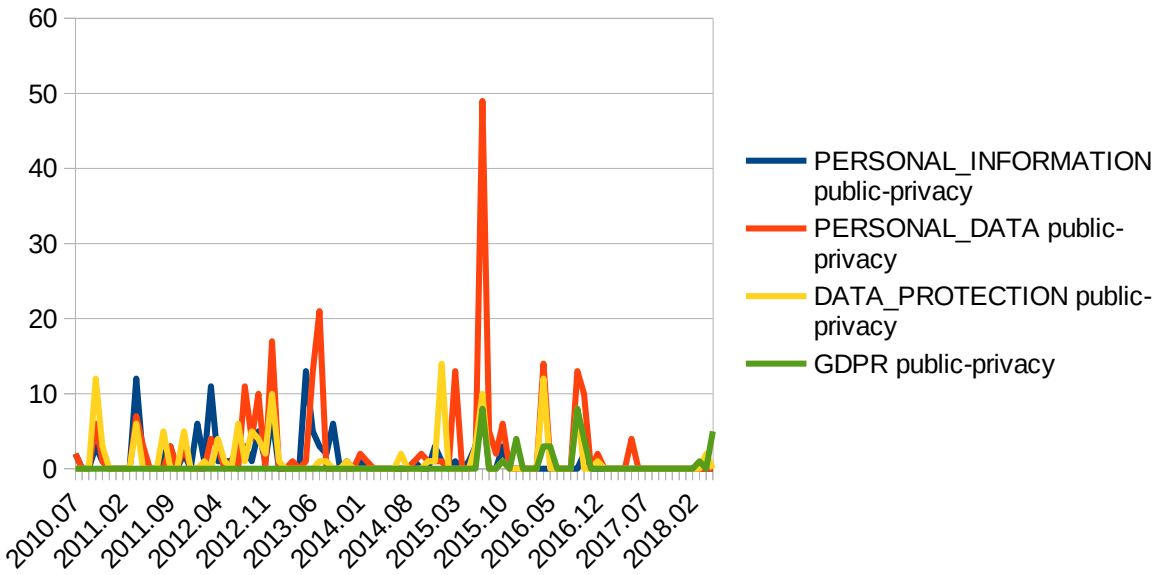
18 An act to amend Section 22575 of the Business and Professions Code, relating to consumers. Approved on 27 September 2013.

19 It states that: "The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties."

20 See all versions since the one published on 13 March 2012: https://www.w3.org/TR/2012/WD-tracking-dnt-20120313/

Convention 108[21], and may be considered a semantic equivalent to the lengthier definition contained in the GDPR (Rossi, 2020). As it turns out, privacy advocates within the W3C, even those who are not trained in the field of law, have often read or listened to what legal experts in Europe and in the United States have written on the topic. This has contributed to an understanding of "privacy" that is in line with the liberal paradigm on privacy which prevails in institutional state-centred settings like the EU (see: Bennett & Raab 2003 and Rossi 2020).

On this topic, it is interesting to note that there has been a gradual shift, within the *public-privacy* mailing-list, from using the term "personal information" to using "personal data". The former is usually found in American legal documents, alongside "personally identifying information", whereas the latter is found more often in European texts. This rise of the "personal data" and the decline of "personal information" appears to be in part – although not completely – linked to the appearance of discussions on the "GDPR" in the mailing-list. This trend can be observed in the following graph, which shows the evolution of the monthly occurrences of each term in e-mails shared on *public-privacy* between its creation and February 2018:



Number of monthly occurrences of the "personal information", "personal data", "gdpr" and "data protection" on the mailing-list of the W3C Privacy Interest Group (Rossi, 2020, p. 562).

This shows that there has been a trend where EU law has become increasingly influential in debates about privacy within the W3C after the adoption of the GDPR. But the relation between techno-policy standards like Do Not Track and legal instruments remains more complex than a gradual domination of the law over standards.

21 Which both define it as "[…] any information relating to an identified or identifiable individual […]" (art. 2 (a) of Convention 108, art. 1 (b) of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data).

On the Relationship Between Legal Instruments and Privacy Techno-Policy Standards

California made it compulsory in 2013 for websites to disclose whether they respect user wishes expressed through Do Not Track. The European Union has taken a more technology-neutral stance, and legal documents, such as the e-Privacy Directive and the proposed e-Privacy Regulation only talk about "appropriate technical settings of a software application enabling access to the internet", "where technically possible and feasible"[22]. Such settings do not necessarily have to be based on Do Not Track, but this mechanism was explicitly mentioned in the proposed Regulation's explanatory memorandum, and has received support both from EU and US legislators and regulators.

This shows that there appears to be a willingness from the side of legislators to leave some implementing decisions to private IG bodies like the W3C, putting the latter into a position that is typically that of a government adopting decrees specifying legislative provisions. Seen from this perspective, techno-policy standards like Do Not Track are *subordinated*, in the legal hierarchy of norms, to the will of the legislator. However, the fact that Do Not Track is global, but legislations are not, blurs this picture significantly. Not *all* legislators are equal in their capacity to set the regulatory framework specification authors take into account. In fact, Irene Kamara and Eleni Kosta (2016) have pointed out several challenges Do Not Track has to overcome to be considered a valid expression of consent even under the data protection legal framework of the EU.

In 2015, Isabelle Falque-Pierrotin, who succeeded Jacob Kohnstamm as chairwoman of the Article 29 Working Party, sent a letter to the TPWG, with two participants who were also privacy advocates (Rob van Eijk and Nick Doty) in copy, with a list of requirements the Do Not Track specifications had to follow in order for them to become a valid standard for the expression of consent to tracking under EU law (Falque-Pierrotin, 2015). Most of her recommendations were not taken over in the specifications. For example, the Article 29 Working Party noted that "the limitation of DNT to only third party tracking presents [a] crucial obstacle, where DNT would not suffice to achieve compliance with the EU legal framework" (Falque-Pierrotin, 2015, p. 2). So despite the fact that European legislation had an influence on the content of techno-policy standards like Do Not Track, and despite the use of arguments based on European law by certain actors in the process, the contents of the Do Not Track specifications cannot be understood as simply an enforcement measure of European privacy and data protection law, or any other law from any other jurisdiction.

Therefore, even if some laws make direct or indirect references to techno-policy standards, the very fact that laws are territorial whereas Internet standards are global makes it impossible to fit the latter into the hierarchy of norms of the former. After all, generally, international treaties and norms are – at least in theory – superior to national law, which are in turn superior to sub-national legislation. But it would not be easily conceivable for global Internet standards to be above national law from a legal standpoint. Stating one applies Do Not Track could not constitute a defence against the established fact of having infringed upon applicable national data protection or privacy legislation applicable where the defendant is located.

22 Art. 9 (2) of the Proposed e-Privacy Regulation, EU Commission, document COM(2017) 10 final

P3P and Do Not Track ultimately failed in being widely accepted and implemented standards. Others, like HTTPS or – to a lesser extent – the IAB's TCF framework for cookie banners, have been successful in imposing their rules to a wide range of Web actors. They have become, or are becoming, effective governance instruments on the Internet, regardless of whether they reflect rules contained in national laws or not. But, like Do Not Track and the TCF, these standards may not have been written were it not for the existence and the influence of these national laws. And while – from an EU perspective – data controllers may not be able to rely only on these standards, they may still use them for compliance as long as they interpret the contents of these standards under the light of their legal obligations when designing their implementations.

Conclusion

The law is thus never as far away as it seems, even in private technical standards-setting bodies that were set up as a reaction to "kings, presidents and voting" to promote "rough consensus and running code". While some of the interviewed participants perceive their work as "reasonably far away from the law", there are many examples of messages containing legal arguments or references to legal expertise being exchanged on W3C mailing-lists related to privacy. EU law, in particular, appears to have become increasingly influential and some terms and definitions, like "personal data" or "controller", have been imported in IETF and W3C documents. Privacy advocates, in particular, have been using the need for compliance with national laws, and especially with EU law since the entry into application of the GDPR, to defend their arguments. While debates on values and politics are frowned upon in arenas that value technical consensus as a guiding principle in the standard-setting process, legal arguments were accepted and there are examples of debates between TPWG participants on points of legal expertise.

Support from both legislators (like Jan Philipp Albrecht, rapporteur of the GDPR in the European Parliament) and regulators (especially the FTC and the Article 29 Working Party) has played an important role in ensuring that progress was made within the W3C on the Do Not Track project. Some project participants were even employed by supervisory authorities. Their combined support, which included direct and indirect references to the project in legislative texts, was decisive in getting the W3C's Director Tim Berners-Lee to extend the TPWG's charter several times, and refocus it on compliance with EU law. This also shows that standards, and in turn the running code implementing them, are influenced by legislative instruments.

Furthermore, there are example of laws making either explicit or implicit making references to techno-policy standards. This opens the possibility of including these instruments in the legal hierarchy of norms, as implementing measures, as long as they can be and are interpreted in a way that is compatible with all other existing legal obligations.

Web specifications studied in this paper were however not influenced by just any legislative instruments. Only laws from a few powerful jurisdictions – in this case, the U.S. and the E.U. – were of influence in this case study. Even then, this influence did not translate into full alignment of the specifications with any given legal order. Bodies like the W3C are under no legal obligation to produce standards that are in alignment with legislative instruments, and even the Article 29 Working Party was not able to impose its choices upon the TPWG. And websites or other implementers are under no obligation to abide by W3C recommendations.

This means that there are a variety of competing policy instruments aiming at regulating privacy on the Web. Whereas P3P and Do Not Track have remained marginal, the IAB has since then developed its own competing standard, called TCF, which is gaining traction as it is implemented by a growing number of Consent Management Platforms used by many websites, despite the criticism it has attracted for insufficiently protecting privacy and data protection rights protected by EU law. But the TCF was created in response to, among others, the entry into application of the GDPR. So in practice, it is difficult to say whether it is the law or competing technical standards and the software that implement them that ultimately rule the Web.

As a conclusion, the relation between techno-policy standards in the field of Web privacy and legal instruments is still complex and troubled. But be it as it may, at least in the field of privacy and despite discourses claiming the contrary, the law is definitely not absent from techno-policy standard-setting processes.

Acknowledgments

This research was made possible by funding received from the Université de technologie de Compiègne, and then from Université Rennes 2. I would also like to thank the members of the Privacy Interest Group and the Tracking Protection Working Group who agreed to being interviewed, as give special thanks to Tara Whalen, co-chair of the Privacy Interest Group, for having agreed to invite me at the 2018 Face-to-Face meeting of the group.

References

Austin, J. (1962). *How to Do Things with Words by J. L. Austin*. Oxford University Press.

Badouard, R., Mabi, C., & Sire, G. (2016). Beyond “Points of Control”: Logics of digital governmentality. *Internet Policy Review*, *5*(3). https://policyreview.info/articles/analysis/beyond-points-control-logics-digital-governmentality

Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

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

Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. MIT Press.

Bennett, C. J., & Raab, C. D. (2003). *The Governance of Privacy. Policy Instruments in Global Perspective*. Ashgate.

Borraz, O. (2005). Chapitre 3: Les normes. In P. Lascoumes & P. Le Galès (Eds.), *Gouverner par les instruments* (pp. 123–161). Presses de Sciences Po. https://www.cairn.info/gouverner-par-les-instruments--9782724609492-page-123.htm

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Butler, J. (1997). *Excitable speech: A politics of the performative*. Routledge.

Butler, J. (2010). Performative Agency. *Journal of Cultural Economy*, *3*(2), 147–161. https://doi.org/10.1080/17530350.2010.494117

Celeste, E. (2018). *Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges* (SSRN Scholarly Paper ID 3219905). Social Science Research Network. https://doi.org/10.2139/ssrn.3219905

Contreras, J. L. (2016). *Patents and Internet Standards* (No. 29; Global Commission on Internet Governance - Paper Series). Centre for International Governance and Innovation and Chatham House.

Coupez, F., & Péronne, G. (2020). Consentement aux cookies: Quelle est la bonne recette ? *Droit de La Propriété Intellectuelle et Du Numérique*, *3*, 189.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Proceedings 2019 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2019.23378

Dehousse, R. (2005). Chapitre 9 : La méthode ouverte de coordination. Quand l'instrument tient lieu de politique. In P. Lascoumes & P. Le Galès (Eds.), *Gouverner par les instruments* (pp. 331–356). Presses de Sciences Po; Cairn.info. https://www.cairn.info/gouverner-par-les-instruments--9782724609492-p-331.htm

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

Doty, N. (2015). Reviewing for Privacy in Internet and Web Standard-Setting. *2015 IEEE Security and Privacy Workshops*, 185–192. https://doi.org/10.1109/SPW.2015.18

Doty, Nick, & Mulligan, D. K. (2013). Internet Multistakeholder Processes and Techno-Policy Standards. *Journal on Telecommunications and High Technology Law*, *11*, 135–184.

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

Fraenkel, B. (2006). Actes écrits, actes oraux: La performativité à l’épreuve de l’écriture. *Études de communication*, *29*, 69–93. https://doi.org/10.4000/edc.369

Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*. https://doi.org/10.1108/14779961111191039

Gougeon, P. (1995). «Nul n’est censé ignorer la loi». La publication au Journal officiel: Genèse d’un mode d’universalisation de la «puissance publique». *Politix. Revue des sciences sociales du politique*, *8*(32), 66–88. https://doi.org/10.3406/polix.1995.2090

Hondius, F. W. (1975). *Emerging data protection in Europe*. Elsevier.

Jabłonowska, A., & Michałowicz, A. (2020). Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User’s Consent to the Storage of Cookies (C-673/17 Planet49). *European Data Protection Law Review*, *6*(1), 137–142. https://doi.org/10.21552/edpl/2020/1/19

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.

Kohnstamm, J. (2012). *Letter to Alain Heureux and Angela Mills-Wade. Ref. Ares(2012)240896*. Article 29 Working Party. http://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120301_reply_to_iab_easa_en.pdf

Lascoumes, P. (2004). La Gouvernementalité: De la critique de l’État aux technologies du pouvoir. *Le Portique*, *13–14*. https://leportique.revues.org/625

Lascoumes, P., & Le Galès, P. L. (2005a). Conclusion: De l’innovation instrumentale à la recomposition de l’Etat. In P. Lascoumes & P. Le Galès (Eds.), *Gouverner par les instruments* (pp. 357–370). Presses de Sciences Po. https://www.cairn.info/gouverner-par-les-instruments--9782724609492-page-11.htm

Lascoumes, P., & Le Galès, P. L. (2005b). Introduction: L’action publique saisie par ses instruments. In P. Lascoumes & P. Le Galès (Eds.), *Gouverner par les instruments* (pp. 11–44). Presses de

Sciences Po. https://www.cairn.info/gouverner-par-les-instruments--9782724609492-page-11.htm

Laugier, S. (2004). Performativité, normativité et droit. *Archives de Philosophie*, *Tome 67*(4), 607–627.

Lavelle, S. (2009). Politiques des artefacts.: Ce que les choses font et ne font pas. *Cités*, *39*(3), 39. https://doi.org/10.3917/cite.039.0039

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.

Lessig, L. (2000, January 1). *Code Is Law*. Harvard Magazine. http://harvardmagazine.com/2000/01/code-is-law-html

Massit-Folléa, F. (2014). La régulation de l'internet: Fictions et frictions. In M. Carmes & J.-M. Noyer (Eds.), *Les débats du numérique* (pp. 17–45). Presses des Mines. http://books.openedition.org/pressesmines/1661

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. *ArXiv:1911.09964 [Cs]*. http://arxiv.org/abs/1911.09964

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

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376321

Ollivier-Yaniv, C. (2018). Présentation du dossier. *Politiques de communication*, *N° 11*(2), 5–14.

Reidenberg, J. (1997). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, 553–593.

Rossi, J. (2020). *Protection des données personnelles et droit à la vie privée: Enquête sur la notion controversée de «donnée à caractère personnel»*. Université de technologie de Compiègne.

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., Bielova, N., & Matte, C. (2019). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *ArXiv:1912.07144 [Cs]*. http://arxiv.org/abs/1912.07144

Schwartz, P. M., & Solove, D. (2012). *PII 2.0: Privacy and a New Approach to Personal Information; Privacy and Security Law Report, 11 PVLR 142*. https://works.bepress.com/paul_schwartz/109/

Sire, G. (2017). Gouverner le HTML. *Réseaux*, *206*, 37–60. https://doi.org/10.3917/res.206.0037

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

Tréguer, F. (2019). *L'utopie déchue: Une contre-histoire d'Internet, XVe-XXIe siècle*. Fayard.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19),*. https://doi.org/10.1145/3319535.3354212

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121–136.

Zittrain, J. (2003). Internet Points of Control. *Boston College Law Review*, *44*(2), 653–688.

Zuiderveen Borgesius, F. J. (2016). Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review*, *32*(2), 256–271. https://doi.org/10.1016/j.clsr.2015.12.013

Case law

ECJ 17 December 1970 Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, case 11-70.

BVerfG, Judgment of the Second Senate of 05 May 2020 - 2 BvR 859/15

Legal References

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981 (Convention 108)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

An act to amend Section 22575 of the Business and Professions Code, relating to consumers. Approved on 27 September 2013. (California)

Regulation 2016/679/EU of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Quoted E-Mails

Name of the sender	**Date**	**URL**
Aleecia McDonald	19 December 2016	https://lists.w3.org/Archives/Public/public-tracking/2016Dec/0025.html
Thomas Roessler	12 May 2009	https://lists.w3.org/Archives/Public/public-geolocation/2009May/0025.html
Ninja Marnau	30 November 2011	https://lists.w3.org/Archives/Public/public-tracking/2011Nov/0288.html
Shane Wiley	30 November 2011	https://lists.w3.org/Archives/Public/public-tracking/2011Nov/0290.html
Jonathan Mayer	10 December 2011	https://lists.w3.org/Archives/Public/public-tracking/2011Dec/0056.html
Rigo Wenning	12 January 2012	https://lists.w3.org/Archives/Public/public-tracking/2012Jan/0107.html
Jacob Simpson	5 March 2012	https://lists.w3.org/Archives/Public/public-tracking/2012Mar/

		0058.html
Jeff Jaffe	16 December 2016	https://lists.w3.org/Archives/Public/public-tracking/2016Dec/0017.html
Aleecia McDonald	16 December 2016	https://lists.w3.org/Archives/Public/public-tracking/2016Dec/0020.html
Mike O'Neill	16 December 2016 (1)	https://lists.w3.org/Archives/Public/public-tracking/2016Dec/0014.html
Mike O'Neill	16 December 2016 (2)	https://lists.w3.org/Archives/Public/public-tracking/2016Dec/0018.html
Matthias Schunter	16 December 2016	https://lists.w3.org/Archives/Public/public-tracking/2016Dec/0016.html
Walter van Holst	16 December 2016	https://lists.w3.org/Archives/Public/public-tracking/2016Dec/0019.html
Rob van Eijk	28 March 2017	https://lists.w3.org/Archives/Public/public-tracking/2017Mar/0032.html
Xueyuan Jia	10 April 2018	https://lists.w3.org/Archives/Public/public-tracking/2018Apr/0002.html
Xueyuan Jia	17 January 2019	https://lists.w3.org/Archives/Public/public-tracking/2019Jan/0000.html

W3C Documents (Including Specification)

Dawson F. (ed) (28 June 2013) *Specification Privacy Assessment (SPA) Creating Privacy Considerations for W3C Technical Specifications*, W3C PING. https://yrlesru.github.io/SPA/

Doty N., West H., Brookman J., Harvey S., Newland E. (eds) (22 January 2019) *Tracking Compliance and Scope*, W3C TPWG. https://www.w3.org/TR/tracking-compliance/

Doty, N. (ed) (26 March 2020). *Mitigating Browser Fingerprinting in Web Specifications*. W3C PING (26 March 2020) https://w3c.github.io/fingerprinting-guidance/

Fielding, R. & Singer D. (eds) (17 January 2019) *Tracking Preference Expression (DNT)*, W3C TPWG. https://www.w3.org/TR/tracking-dnt/

O'Connor, T., Snyder P., Novak J., Olejnik L. & West M. (eds) (17 June 2020) *Self-Review Questionnaire: Security and Privacy* . W3C PING and TAG. (17 June 2020) https://web.archive.org/web/20200704082104/https://w3ctag.github.io/security-questionnaire/

Popescu A. (ed) (8 November 2016) *Geolocation API Specification 2nd Edition*, W3C Geolocation Working Group. https://www.w3.org/TR/geolocation-API/

Tschofening, H. & Doty N. (eds) (28 July 2020), *Privacy Considerations for Web Protocols*. W3C PING. https://w3c.github.io/privacy-considerations/

Wenning R. & Schunter M. (eds) (13 November 2006) *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*, W3C P3P. https://www.w3.org/TR/P3P11/

Other Documents

EU Commission. 10 January 2017. *Proposal for a Regulation of the European Parliament and 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)*. Document COM(2017) 10 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

FTC, 2011. *A Word from Washington about Behavioral Advertising and Do Not Track*, communiqué de presse du 8 mars. Disponible en ligne à l'URL : https://www.ftc.gov/sites/default/files/documents/public_statements/word-washington-about-behavioral-advertising-and-do-not-track/110308forasspeech.pdf (document consulté le 20 décembre 2019)

Falque-Pierrotin, I. 1st October 2015. Article 29 Data Protection Working Party comments in response to W3C's public consultation on the W3C Last Call Working Draft, 14 July 2015, Tracking Compliance and Scope. Available on-line: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20151001__letter_of_the_art_29_wp_w3c_compliance.pdf

Kohnstamm, J., 1 March 2012, *Letter to Alain Heureux and Angela Mills-Wade, OBA Industry*.

https://ec.europa.eu/justice/article-29/documentation/other-document/files

2012/20120301_reply_to_iab_easa_en.pdf