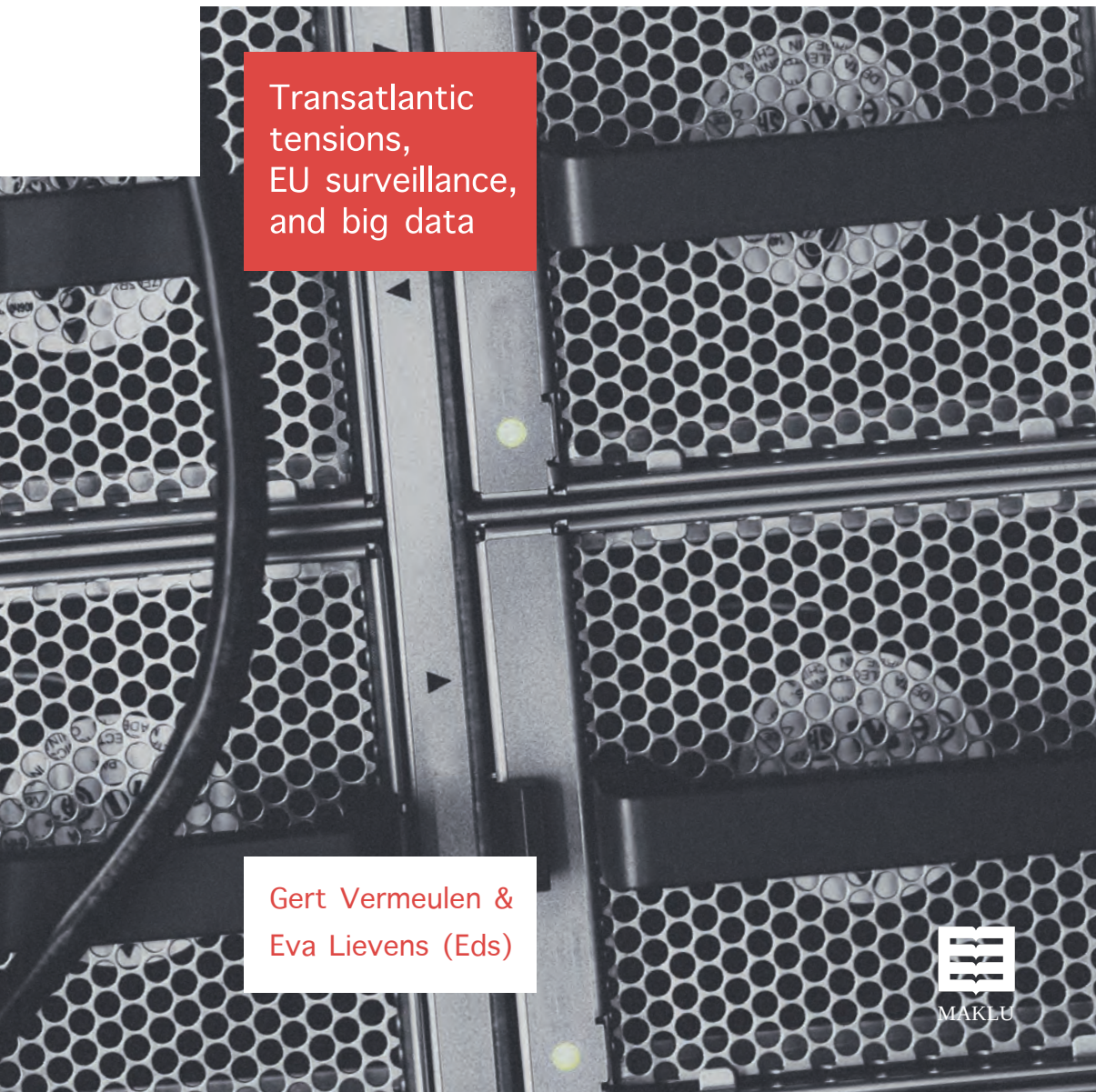
Data Protection and Privacy under Pressure



Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen &
Eva Lievens (Eds)

MAKLU

Data Protection and Privacy under Pressure

Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen
Eva Lievens
(Eds)

Maklu

Antwerp | Apeldoorn | Portland

Data Protection and Privacy under Pressure
Transatlantic tensions, EU surveillance, and big data
Gert Vermeulen and Eva Lievens (Eds)
Antwerp | Apeldoorn | Portland
Maklu
2017

341 p. – 24 x 16 cm
ISBN 978-90-466-0910-1
D/2017/1997/89
NUR 824

Maklu-Publishers
Somersstraat 13/15, 2018 Antwerp, Belgium, info@maklu.be
Koninginnelaan 96, 7315 EB Apeldoorn, The Netherlands, info@maklu.nl
www.maklu.eu

USA & Canada
International Specialized Book Services
920 NE 58th Ave., Suite 300, Portland, OR 97213-3786, orders@isbs.com,
www.isbs.com

Back to Yahoo!?

Regulatory clashes in cyberspace in the light of EU data protection law

ALBERTO MIGLIO[1]

The implementation of the *Google Spain* judgment of the Court of Justice of the European Union raises issues largely similar to those prevailing in the debate on the regulation of Internet content in the late 1990s and 2000s. By looking at the most famous case from that period, this contribution discusses what lessons, if any, can be learnt from that debate. It argues that while geographic filtering, which the 2000 *Yahoo!* case endorsed as a technique for the regulation of online activities, represents a valid model for dealing with delisting of online search results, in this context any one-size-fits-all approach would have serious shortcomings. However, in turn, the quest for more flexible approaches raises concerns that regulators, courts and businesses will have to address.

1. INTRODUCTION

Controversial as it was, the judgment of the Court of Justice of the European Union in *Google Spain,*[2] which rather imprecisely dubbed 'the judgment on the right to be forgotten',[3] was widely and immediately perceived as a landmark case that would shape how we deal with the Internet.[4]

Requiring search engines to take down URLs containing personal data of which the processing does not (or no longer) comply with EU data protection law is undoubtedly of significant practical importance for individuals seeking

[1] Postdoc fellow, Law Department, University of Turin. Email: alberto.miglio@unito.it.

[2] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos* (AEPD) *and Mario Costeja González* EU:C:2014:317.

[3] For criticism see Orla Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78 Modern Law Review 522, 528.

[4] See Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos*' (2014) 14 Human Rights Law Review 761; Christopher Rees and Debbie Heywood, 'The 'right to be forgotten' or the 'principle that has been remembered'' (2014) 30 Computer Law and Security Review 574, 577.

to keep control over the spread of personal data across the web. This is demonstrated by the high number of requests for delisting addressed to Google, that in May 2017 reported having evaluated 720,000 applications in three years, removing around 43 percent of the more than 2 million links submitted. [5]

Perhaps even more important, the judgment's significance is demonstrated by the ongoing lively debate that it has generated on the protection of fundamental rights online and on the application of EU data protection law. Aside from the controversial character of some of the Court's findings – such as the qualification of search engines as data controllers [6] or the conclusion that Google Inc.'s data processing fell within the scope of the EU data protection law despite being carried out in a third country – and the widespread criticism it received especially from the US,[7] it is the questions the judgment left open that have continued to provide food for thought for academics, practitioners and citizens alike.

Indeed, considering it represented a first step in a new direction, the judgment has raised a number of questions that are complicating its implementation and are calling for further judicial clarification.[8] Some of those questions relate to the actual process of sorting information that has to be delisted. Who should decide and under which supervisory mechanisms? How should this process be conducted? When should information be considered inadequate, irrelevant or no longer relevant or excessive and therefore be removed? How should search engines balance the protection of privacy and freedom of expression?[9]

Arguably the most contentious issue that has surfaced in the implementation of delisting, however, is the geographic scope of the obligation to remove

---

[5] Peter Fleischer (Google's Global Privacy Counsel), 'Three years of striking the right (to be forgotten) balance' (*Google in Europe*, 15 May 2017) <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/>.

[6] For a critical appraisal see Giovanni Sartor, 'Search Engines as Controllers. Inconvenient Implications of a Questionable Classification' (2014) 21 MJ 564.

[7] See, for instance, John W. Kropf, 'Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD). Case C-131/1' (2014) 108 AJIL 502.

[8] Indra Spiecker, 'A New Framework for Information Markets: *Google Spain*' (2015) 52 Common Market Law Review 1033, 1039.

[9] The Court of Justice will soon have to deal with some of these questions in the context of a reference from a preliminary ruling proposed in February 2017 by the French Council of State: Conseil d'Etat, order of 24 February 2017, Mme C, M. F, M. H, M. D., applications Nos 391000, 393769, 399999, 401258.

search results. This is a different question than the one relating to the personal scope of application of the Data Protection Directive. The Court of Justice made clear in *Google Spain* that the Directive applies to data controllers established in third countries as long as they have an establishment on EU territory for the promotion and sale of advertising space. Although this statement is certainly a source of tensions in transatlantic relations and is viewed – improperly perhaps – as a claim to extraterritorial jurisdiction, the key question relating to the geographic scope of the 'right to be forgotten' is another one, namely whether a search engine operator should delist results on a local or global scale.

Whereas its application to search engines for purposes of data protection may be a novelty triggered by the CJEU's finding that search engine operators are data controllers within the meaning of the Data Protection Directive, the underlying problem is a classic one and is well-know to anyone having even a limited familiarity with jurisdictional claims in cyberspace.[10] It is the question of determining the scope of application of local laws in the online environment and the ways of their enforcement.

Indeed, the rise of the Internet made the quest for jurisdictional criteria applicable to online activities a major problem of cyber law. While the borderless structure of the web made content published online ubiquitous and in principle accessible from anywhere in the world, States have attempted to regulate online activities by enforcing local laws, which often considerably diverge from one another. This phenomenon has generated jurisdictional conflicts and powerfully revived the academic debate on international law limits to jurisdiction.

Against this background, the contribution addresses the following question: What lessons, if any, can be learnt for EU data protection law from the scholarly debate and the case law that developed in the late 1990s and in the 2000s in the context of the regulation of web-based content? The contribution attempts to answer this question by exploring the similarities between the implementation of delisting under the EU Data Protection Directive and the *Yahoo!* Case,[11] which is by far the most famous example of litigation concerning the enforcement of local laws against global Internet service providers (ISPs).

---

[10] Orla Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78 Modern Law Review 522, 531.

[11] Tribunal de Grande Instance de Paris, order of 22 May 2000, *UEJF and Licra v Yahoo! Inc and Yahoo! France*. For an interesting account of the case see Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).

2. JURISDICTIONAL CONFLICTS IN CYBERSPACE: YAHOO!

When in May 2000 a French court enjoined *Yahoo!*, a US-based ISPs, to enforce restrictions on the access to web content that infringed French law, the decision provoked an outcry overseas and started a complex jurisdictional conflict.

The case originated from a lawsuit two French NGOs filed against *Yahoo! Inc*. in the *Paris Tribunal de Grande Instance*. The plaintiffs complained that Nazi memorabilia, of which the display is prohibited by French law, were offered for sale on an auction web page operated by *Yahoo!,* and sought an injunction prohibiting the defendant from offering such items for sale in France. In its defence, *Yahoo!* challenged the jurisdiction of the French court and argued that compliance with French law would require the worldwide removal of the contentious web page, thereby infringing the right to free speech *Yahoo!* and its users enjoyed under the First Amendment to the US Constitution. After finding that it had jurisdiction to hear the claim since the harm was produced in France, the *Tribunal de Grande Instance* requested an opinion from an international team of experts as to whether it was technically feasible to block users based in France from accessing the contentious web page. The experts concluded that the then current state of technology would allow *Yahoo!* to implement a geographically selective blocking with an estimated success rate of approximately 90 percent. Based on this finding, the court ordered *Yahoo!* to block access from France to the content which infringed French law. Despite suing the plaintiffs in California seeking a declaratory judgment preventing the French order from being enforced in the US, faced with the prospect of substantial fines in case of non-compliance, *Yahoo!* eventually relented and even banned Nazi memorabilia from its auction sites altogether.

Yahoo! is undoubtedly the most widely discussed case on Internet jurisdiction, as it is cited in virtually every publication on the subject as the foremost example of the interplay of conflicting public policies in the online world.[12] In *Yahoo!*, the conflict involved the constitutional protection of free speech and

[12] See Paul Schiff Berman, 'The Globalization of Jurisdiction' (2002) 151 Pennsylvania Law Review 311, 327; Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006), 1; Bernard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IJLIT 142; Andreas Manopoulos, 'Raising 'Cyber-Borders': The Interaction Between Law and Technology' (2003) IJLIT 40; Joel Reidenberg, 'Technology and Internet Jurisdiction' (2005) 153 University of Pennsylvania Law Review 1951; Mathias Reimann, 'Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage' (2002-2003) 24 Michigan Journal of International Law 663, 665; Georgios I Zekos, 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction' (2007) 15 IJLIT 1.

the safeguard of democratic values underpinning the prohibition of Nazi apology. As the same activity was illegal under French law but enjoyed constitutional protection in the US, the case exemplified the potential of the web to give rise to regulatory clashes. Justifying the assertion of prescriptive jurisdiction by multiple States, the borderless nature of the Internet made such clashes all the more likely.

Therefore, it is not surprising that the French court's decision in the *Yahoo!* case was highly controversial and met with considerable criticism especially in the US.[13] Some authors feared that imposing an obligation on ISPs to comply with local laws would force Internet service providers to adapt to the most restrictive standard imposed by any national law in order to avoid liability.[14] Freedom of expression and the then popular idea of the Internet as a global free space would suffer as a result.

In fact, this reading of the case omits to consider one key aspect of the order issued by the French court. While finding that *Yahoo!* had to comply with French law, the court did not impose worldwide compliance by banning Nazi-related items from its auction website altogether. By contrast, it merely requested *Yahoo!* to filter access to the relevant content based on the physical location of surfers. This could be done through geographic filtering technology, which by identifying the physical location of devices accessing the network would allow a 'zoning'[15] of the web.

Far from representing an instance of exorbitant jurisdiction – a view many held even on this side of the Atlantic[16] – the Paris court's decision in fact exemplified a pluralistic approach to the regulation of the Internet. As Professor Muir-Watt noted in a commentary on the *Yahoo!* case, the possibility offered by technology to filter content based on the location of Internet-connected terminals provided for a legitimate and practical solution for regulatory conflicts in cyberspace.[17] 'Zoning' through geolocation and geographic filtering

---

[13] See, for instance, Ben Laurie, 'An Expert's Apology' (21 November 2000) <http://apache-ssl.securehost.com/apology.html>.

[14] Thomas Schultz, ''Carving up' the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 812-813.

[15] For this expression see L. Lessig, A. Resnick, 'Zoning Speech on the Internet: A Legal and Technical Model', (1999) 98 Michigan Law Review 395.

[16] See Daniel Arthur Laprès, 'L'exorbitante affaire Yahoo' (2002) Journal de droit international 975.

[17] Horatia Muir Watt, 'Yahoo! Cybercollision of Cultures: Who Regulates?' (2002-2003) 24 Michigan Journal of International Law 273, esp 379-289; cf also Joel

would allow for the coexistence of a plurality of regulatory spaces within the web, each of which could reflect different policy choices. On the one hand, this would prevent the circumvention of local laws. On the other hand, it would still be possible for transnational ISPs to offer their services across different jurisdictions without having to comply with the requirements of all local laws *simultaneously*: they would *merely* have to differentiate the content that would be accessible to surfers in different countries by resorting to filtering.

3. TERRITORIAL SCOPE OF DELISTING SEARCH RESULTS UNDER EUROPEAN DATA PROTECTION LAW: THREE ALTERNATIVES

Almost two decades after the *Paris Tribunal de Grande Instance* issued its order in the *Yahoo!* case, the *Google Spain* judgment has marked the emergence of a similar clash between competing views on the balancing of constitutional values on the Internet[18] and the debate on the extension of the obligation to delist search results under EU law closely resembles discussions on Internet jurisdictions that were popular in the early-mid 2000s.

When it has been established that a request for delisting personal data made by a data subject should be granted, there are three possible ways for a search engine operator to implement it.

a) The first option consists of applying the delisting only to the national domain(s) of the search engine website corresponding to the Member State concerned or to all Member States of the European Union. In the case of Google, if a request for delisting is made, say, from Belgium, this means that Google would delist the data on google.be and possibly also on other EU domains such as google.fr, google.de, google.it etc. By contrast, users would still be able to access the original information by typing the same query on google.com or any non-European country domain of the Google search engine.

Not surprisingly, this has been the solution preferred and originally implemented by Google when dealing with delisting requests in the aftermath of the *Google Spain* ruling. It has also been endorsed by the the Advisory Council to Google on the right to be forgotten.[19]

Reidenberg, 'Yahoo and Democracy on the Internet' (2002) 42 Jurimetrics 261, 271-275.

[18] Christopher Kuner, 'Google Spain in the EU and International Context' (2015) MJ 158, 159.

[19] See Advisory Council to Google on the Right to be Forgotten, Final Report (6 February 2015) 20.

In order to justify its choice, Google provided statistical data showing that more than 95% of all queries originating in Europe are made through local versions of the search engine, with onlyvery few EU-based users resorting to google.com for their searches. The problem with those data, however, is that these are aggregated data that cover all Google searches. By contrast, Google has not provided any data showing that this pattern is also true for *name* queries – the only searches to which delisting applies.

In any event, whether or not searchers are more likely to switch to google.com for personal name searches than for other queries, the problem with delisting limited to some national domains of the search engine is that this approach is open to easy circumvention.[20] Most Internet users are aware that it suffices a click at the bottom of the page to switch from, say, google.be to google.com. In addition, when a request for delisting has been granted a notice at the bottom of the page informs users that 'some results may have been removed under data protection law in Europe', possibly prompting curious surfers to look for the missing information on other versions of the search engine. In light of these circumstances, delisting search results only on some national domain of Google Search without any additional measure can hardly be considered an adequate safeguard for the right of data protection.

b) Global delisting. Alternatively, the search engine operator could be required to de-index search results globally, removing the relevant personal data from all versions of its engine and making it effectively impossible to access from anywhere in the world. Proponents of this approach include notably the French data protection authority (CNIL) and the Article 29 Working Party. They argue that global delisting is necessary to ensure effective protection of the data subject's right to privacy.

In its 2014 Guidelines on the implementation of the *Google Spain* judgment, the Article 29 Working Party emphasised that limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains does not satisfactorily guarantee the rights of data subjects and therefore does not amount to a correct implementation of the Court of Justice's ruling. It added that in order to provide effective and complete protection of the data subject's rights, delisting would have to be 'effective on all relevant domains, including .com'.[21] While this statement leaves open two

[20] See Emmanouil Bougiakiotis, 'The Implementation of the Google Spain Ruling' (2016) 24 IJLIT 311, 325.

[21] Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc v Agencia

important questions – namely what is needed to make delisting *effective* and whether third county national domains also qualify as 'relevant domains' in addition to .com[22] – the dominant view is that the Working Party advocates global delisting.[23] The French data protection authority in particular has been a vocal proponent of this approach[24] and has challenged Google's policy on several occasions.[25]

Global delisting, however, is often criticised as implying a disproportionate expansion of the EU's jurisdiction and possibly a breach of international law.[26] In addition, it is often viewed as a highly unpractical solution that could trigger an international clash.[27]

c) Finally, a third option is 'zoning' by geographic filtering. According to this model, while delisting does not affect non-European domains of the search

Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12 (adopted on 26 November 2014) 14/EN WP 225, 3.

[22] On the uncertainty regarding this question see Dan Svantesson, 'Limitless Borderless Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review 116, 120.

[23] See Emmanouil Bougiakiotis, 'The Implementation of the Google Spain Ruling' (2016) 24 International Journal of Law and Information Technology 311, 330. See also Christopher Kuner, 'Google Spain in the EU and International Context' (2015) 22 MJ 158, 160, noting that the DPAs approach 'seems to represent a departure from their former view that the territorial application of EU data protection law should be limited by factors such as proportionality and enforceability'.

[24] In an article published on the French newspaper Le Monde, the president of the CNIL and of the Article 29 Working Party presented several arguments in favour of worldwide delisting: see Isabelle Falque-Pierrotin, 'Pour un droit au déréférencement mondial' (29 December 2016) Le Monde.

[25] See 'CNIL orders Google to apply delisting on all domain names of the search engine' (12 June 2015) <https://www.cnil.fr/fr/node/15790>. For a brief overview of the case law of both civil and administrative courts in France on the right to delisting, see Olivia Tambou, 'Le droit à l'oubli numérique' (2017) 606 Revue de l'Union européenne 156, 160-162.

[26] For a discussion on the EU data protection law in light of international law limits to jurisdiction see Dan Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl L 53; see also the contribution by Brendan Van Alsenoy in this volume.

[27] See Paul De Hert and Vagelis Papakonstantinou, 'Google Spain. Addressing Critiques and Misunderstandings One Year Later' (2015) 22 Maastricht Journal of European and Comparative Law 624, 637.

engine, surfers accessing the Internet from the EU/EFTA territory are prevented from viewing the filtered content whatever version of the engine they are using.

Despite scholarly suggestions that this approach, which corresponds to the solution imposed by the French court in the *Yahoo!* case, could represent a viable option for dealing with delisting,[28] surprisingly it was not initially considered by the major actors involved in the implementation of the *Google Spain* ruling, namely Google and national data protection authorities. On the one hand, Google first only deleted search results on the country domains corresponding to the EU Member States, on the implicit assumption that geographic filtering was not necessary to ensure an effective protection of the data subjects' rights. On the other hand, the Article 29 Working Party did not even discuss whether geographic filtering could constitute an adequate remedy and insisted on delisting on all relevant domains without specifying how it should be implemented.[29]

Eventually, following indications by several national DPAs, in March 2016 Google modified its approach to delisting. In addition to removing search results on all European versions of the search engine, it resorted to geographic filtering by restricting access to the delisted URL on all domains, including google.com, 'when accessed from the country of the person requesting the removal'.[30] Geographic filtering has thus become the practice since.

4. REFERENCE FOR PRELIMINARY RULING FROM THE FRENCH COUNCIL OF STATE

The new approach adopted by Google in dealing with requests and the abandonment of a selection criterion based solely on country domains has not put an end to disputes over the territorial scope of delisting.

Only a few days after Google announced that it would block access to search results based on geolocation, the CNIL adopted a decision sanctioning it for

---

[28] Orla Lynskey, 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78 Modern Law Review 522, 531-532.

[29] Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12 (adopted on 26 November 2014) 14/EN WP 225, 3.

[30] Peter Fleischer 'Adapting our approach to the European right to be forgotten' <https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig/>.

failure to comply with its delisting obligations.[31] The CNIL rejected the approach followed by the search engine operator, pointing at two major shortcomings. First, geographic filtering does not prevent users located in third countries, including individuals having personal or business relationships with the data subject, from viewing the contentious search results. Second, blocking based on surfers location can be circumvented by altering the geographic location of an IP address through a proxy server. Therefore, according to the CNIL geographic filtering does not sufficiently protect the data subject's right to privacy.

Google challenged the CNIL decision before the Council of State, which after hearing the parties stayed the proceedings and request a preliminary ruling from the Court of Justice.[32] The three questions submitted by the referring court all deal with the territorial scope of the delisting obligation and essentially reflect the options outlined in the previous paragraphs.

The first question poses the alternative between global and geographically selective delisting. In other words, the Council of State asked whether the Directive obliges a search engine provider to delist search results on every national domain of the engine, in order to prevent access to the relevant results from any country in the world.

Only in the case of a negative answer to the first question, the second and the third question become relevant. With the second question, the referring court requested clarification as to whether delisting should only target the search engine's domain name corresponding to the country the research is assumed to have been launched from or whether it should extend to the domain names of all 28 European versions of the engine (eg google.be, google.nl, google.fr. etc).

Finally, the third question deals with geographic filtering. If the Directive does not impose global delisting, does it require from search engine operators, in addition to the removal of search results from the European domains, filter-

[31] CNIL 'Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre de Google' (decision of 10 March 2017) <https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu>.

[32] Conseil d'Etat 'Google Inc., application No. 399922' (19 July 2017) <http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC>.

ing based on the location of hardware in order to prevent access to the relevant content from users based in the EU, whichever version of the search engine they use?

5. GEOGRAPHIC FILTERING: THE WAY FORWARD?

Looking at the discussion on the geographic scope of delisting and at the questions referred to the Court of Justice in light of the *Yahoo!* case, suggests that geographic filtering could represent the optimal solution. In *Yahoo!*, geolocation and filtering allowed for the coexistence of different regulatory regimes on a territorial basis, preserving the effectiveness of local law while avoiding unnecessary overreach. Since the implementation of the right to delisting poses a similar problem, this approach could be seen as offering an equal satisfactory solution.

Yet, two major dissimilarities between the *Yahoo!* type of cases and the *Google Spain* type of situations seem to undermine the analogy. The first is the different nature of the underlying policy conflicts. The second is the difference in complexity of the assessment that their required for enforcement.

a) The judgment in *Google Spain* must be read against the background of the strong emphasis the Court has placed on the effective protection of fundamental rights especially after the entry into force of the Lisbon Treaty which transformed the Charter of Fundamental Rights into a binding instrument of primary law. This tendency has been particularly pronounced with respect to data protection,[33] as it is recognised in the Charter as an autonomous right,[34]

[33] See Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23 MJ 812; Maja Brkan, 'The Court of Justice of the EU, Privacy and Data Protection: Judge-made Law as a Leitmotiv in Fundamental Rights Protection' in Maja Brkan, Evangelia Psychogiopoulou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (10 et seq, Elgar, 2017), Selena Crespi, 'Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati' (2015) Rivista italiana di diritto pubblico comunitario 819; Hielke Hijmans, 'Right to Have Links Removed. Evidence of Effective Data Protection' (2014) 21 MJ 555, 556.

[34] Art 8 of the Charter.

and clearly discernible in the case law both prior[35] and subsequent to *Google Spain.*[36]

The judgment itself is based on a teleological reasoning.[37] The Court's analysis and main findings are clearly driven by the concern to ensure that the data subjects' rights are effectively protected and that the safeguards put in place by the legislature are not circumvented.[38]

Defintely other arguments will also play a role when the Court answers the questions raised by the Council of State. Among them is certainly the issue of what limits international law poses to the reach of unilateral regulation of the Internet – a defence that Google has already raised in the domestic proceedings. Yet the Court has so far been cautious in drawing international law limits to the territorial reach of EU measures, and has done so not only in the field of competition law where extraterritoriality has longer been accepted.[39] In the light of precedents, effective protection of the data subject's rights can be expected to play a more prominent role in the Court's analysis. The decisive question is thus likely to be whether filtering, despite its intrinsic geographic limitation and the risk of circumvention through a proxy, offers sufficient safeguards for the data subject's privacy.

Whatever the Court's answer will be, it seems clear that the *Yahoo!* precedent is only of limited use when dealing with data protection issues. Not, however, because it is outdated or no longer offers a valid paradigm for dealing with regulatory conflicts in cyberspace; rather because of the different nature of

---

[35] See eg Joined Cases C-92/09 & C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* EU:C:2010:662 [2010] ECR I-11063; Joined cases C-293/12 é C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] EU:C:2014:238.

[36] See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650; Joined Cases C–203/15 and C–698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson* EU:C:2016:970.

[37] Paul De Hert and Vagelis Papakonstantinou 'Google Spain. Addressing Critiques and Misunderstandings One Year Later' (2015) 22 MJ 624, 629.

[38] *Google Spain*, (n 2) para 54.

[39] To date, the judgment that most comprehensively deals with the extraterritorial application of EU law is Case C-366/10 *American Transport Association of America and Others v Secretary of State for Energy and Climate Change* [2011] EU:C:2011:864 where the Court of Justice upheld the validity of a directive establishing a greenhouse gas emissions trading scheme for the aviation sector.

conflicts that arise in the implementation of data protection law. In other words, it might be easier and more obvious to accept the territorially limited application of a State's public policy choice – such as the prohibition of Nazi apology – than the geographically selective application of a fundamental right.

b) The second problem is that while all relevant actors – Google, the DPAs and the Council of State – assume that one of the three approaches outlined above – territorially selective delisting based on national domains, territorially selective delisting based on geographic filtering or global delisting – must apply to all instances, this is not necessarily the case.

From the viewpoint of search engine operators, the demand for criteria applicable to the generality of cases is perfectly understandable. As any other data controllers under a duty to comply with EU data protection law, they have a strong interest in implementing standards, ideally even automated or semi-automated procedures that would reduce costs. From the perspective of national DPAs, the concern for the maximisation of fundamental rights protection is an equally powerful incentive to advocate global delisting.

Such a one-size-fits-all approach, however, might not be the best way of dealing with requests for de-indexing of web search results. In this respect, the enforcement of a right to data privacy significantly differs from a *Yahoo!* type of situation. In the case of a state policy forbidding, as in *Yahoo!*, the sale of certain items considered illegal under the local law, the prohibition is meant to apply without regard to competing interests and its enforcement usually does not require a great deal of balancing. In addition, once geographic filtering is in place, it does not frustrate the purpose of the French policy that people engage in the commerce of Nazi-related items in the US.

By contrast, when it comes to implementing a right to deleting – or delisting – personal data, the picture is much more complex. As the Court of Justice recognised in *Google Spain*, processing requests for delisting requires a 'fair balance' to be struck between the data subject's fundamental rights to privacy and data protection under Articles 7 and 8 of the Charter of Fundamental Rights and the interest of users in having access to information.[40] Although the Court failed to explicitly recognise it – a failure that has attracted major criticism[41] – the users' 'interest' may also enjoy fundamental right status as

---

[40] Case C-131/12 *Google Spain SL and Google Inc vc Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317, para 81.

[41] See Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos*' (2014) 14 Human Rights Law Review 761, 769.

its preservation is instrumental to guaranteeing the freedom of expression and information. It can be safely assumed that striking a 'fair balance' requires a careful case-by-case assessment and that the relative weight of privacy and competing rights or interests is not always the same. In practice, the outcome of the balancing test could depend on a number of variables, such as the nature of the data (sensitive/non sensitive), whether the information published is false or defamatory, the status and personal condition of the data subject (minors might deserved enhanced protection), whether the data were processed illegally, etc.

It is true that those concerns are already addressed at a different stage, namely when a decision has to be taken on granting a request for delisting in the first place. Nevertheless, they could also affect the desirable geographic scope of delisting.

On the one hand, in certain cases public interest in the availability of information may be strong or even stronger in a third country than within the EU.[42] This problem can be significant in the light of the relatively ill-defined protective scope of the EU data protection rules. Although the Article 29 Working Party has stated that DPAs will deal with claims presenting 'a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State',[43] neither the application of Data Protection Directive nor that of the General Data Protection Regulation (GDPR) that will replace it as of May 2018 are dependent on the nationality or residence of the data subject.[44] As a consequence, at least in theory, EU

[42] Brendan Van Alsenoy and Marieke Koekkoek mention the Mosley case as a good example where there might be a strong interest of users based in third countries in the availability of information (Brendan Van Alsenoy and Marieke Kokkoek, 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to be Delisted'' (2015) 5 IDPL 105, 113.

[43] Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on '*Google Spain and Inc v Agencia Española de Protección de Datos* (AEPD) and *Mario Costeja González*' C-131/12, (26 November 2014) WP 225, 3.

[44] The application of the GDPR is conditional on the data subject being 'in the Union' if the data controller or processor is not established in the Union (Art 4(2)). However, as in the directive this is not a requirement for processing of personal data carried out in the context of an establishment of the data controller or processor on the EU territory (Art 4(1)). In addition, both the Directive and the Regulation contain a recital indicating that the right to the protection of personal data applies 'whatever [the] nationality or residence' of the data subject (recital 2).

data protection law 'could apply to requests for suppression from individuals anywhere in the world'.[45]

On the other hand, the data subject's privacy may will be threathened by physical or legal persons located in third countries. In those cases, geographic filtering can hardly offer an effective remedy. Although not related to personal data, a recent Canadian case offers an interesting illustration of the problem.[46] A Canadian company (Equustek) sued a former distributor, that re-labeled a product and solded it as its own, for breach of intellectual property rights. Equustek won the case, but the infringer relocated its premises to an unknown place and continued to sell its products online. Based on a court order prohibiting the infringer from carrying on business on the Internet, Google de-indexed its web pages, but limited the delisting to google.ca. Equustek then brought court proceedings seeking an injunction requiring Google to delist the infringer's websites from all its search results worldwide. Hearing the case on appeal from Google which had lost before the first instance court, the Supreme Court of Canada delivered a judgment upholding Equustek' right to obtain a global injunction. It noted that the injunction against Google could only attain its purpose if it applied where Google operates, namely globally, and that delisting limited to certain national domains would not prevent harm to the petitioner. Aside from concerns that relate specifically to IP rights – notably in the light of their traditionally territorial character – the judgment illustrates some of the challenges that territorially selective enforcement poses to the effectiveness of rights in the online environment. It is not difficult to imagine cases – as a way of example, one might think of revenge porn of cyberstalking of minors – where the data subject might suffer serious harm from the failure to de-indexing search results on a worldwide basis.

In conclusion, none of the possible approaches to the implementation of delisting seems suitable to apply to all cases. While a selection based on national domains is obviously ineffective and easy to circumvent, global delisting risks being disproportionate and triggering unnecessary jurisdictional conflicts. The 'third way' offered by geographic filtering, although it *generates*

---

[45] Christopher Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges' In Hess B and Mariottini C (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Nomos, 2015) 19, 29; see also Dan Svantesson 'Limitless Borderless Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review 116, 130.

[46] Supreme Court of Canada *Google Inc v Equustek Solutions Inc* [2017] SCC 34.

no interference with the jurisdiction of third countries, may in certain cases be insufficient to effectively protect the rights of the data subject.

6. STRENGTHS AND WEAKNESSES OF A MORE FLEXIBLE APPROACH

In the light of such difficulties, some authors have argued that the territorial scope of delisting under EU data protection law should not necessarily be the same in all circumstances and could vary depending on the nature of data[47] or on a set of substantive factors such as the state interests involved, the likelihood of adverse impact on the data subject in case of territorially selective delisting, the degree of normative convergence between the States involved and the existence of connections with the territory of the forum State.[48] In order to reduce the complexity of a balancing text based on such a variety of substantive factors, other scholars, while still rejecting the assumption that one mode of implementation would work in every case, have suggested adopting geographic filtering as the default approach, while assessing the need for global implementation on a case-by-case basis.[49]

All such attempts at elaborating a nuanced approach to the implementation of the right to delisting are certainly meritorious and would arguably permit a more careful balancing of the rights and interests and stake, in addition to reducing the risk of jurisdictional clashes. However, they also raise two problems that should not be neglected.

a) The first is the need to find a legal basis for any test aimed at determining the scope of delisting on a case-by-case basis. Unfortunately, both the Directive and the GDPR, despite the latter containing specific provisions on the 'right to be forgotten', are completely silent on the territorial scope of application of the duty to delete data that is inadequate, irrelevant or no longer relevant or excessive. As they do not offer any guidance at all as to the scope

[47] Dan Svantesson 'Limitless Borderless Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review 116, 131-134.

[48] Brendan Van Alsenoy and Marieke Koekkoek 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to be Delisted'' (2015) 5 IDPL 105, 116-119.

[49] See Emmanouil Bougiakiotis 'The Implementation of the Google Spain Ruling' (2016) 24 IJLIT 311, 330.

of delisting, *a fortiori* they do not suggest that delisting should have a different scope depending on the kind of information or the interests involved.[50]

The absence of express guidance in the legislative text could certainly be overcome through judicial interpretation. After all, the Court will have to interpret provisions that rely on vague and flexible notions such as 'appropriateness' or 'excessiveness'. In particular, article 12(b) of the Directive mandates rectification or erasure of data 'as appropriate', a criterion that could perhaps be relied upon to legitimise selective delisting.[51] Yet, filling the gap in the legislation through judicial interpretation will require time and create, at least temporarily, legal uncertainty, adding to the many complex questions that already surround the personal and material scope of the 'right to be forgotten' and its implementation.[52] In the meantime, practices developed by data controllers required to enforce request for delisting and the supervision by national DPAs could help devise criteria for determining the territorial requests scope of delisting. In particular, the article 29 Working Party in its advisory function could offer a crucial contribution in this respect.

b) The second problem would be inherent to the rejection of a one-size-fits-all approach and to the search for more flexible solutions. Inevitably, making the scope of delisting dependent on a balancing test would add one further level of complexity to a normative framework that is already highly complex and burdensome to the point of being often perceived as dysfunctional.[53]

Seen from this perspective, the debate on the territorial scope of delisting highlights a dilemma that is not limited to the implementation of the *Google*

---

[50] Against this background, the request for preliminary ruling by the Council of State does not hint at criteria that may suggest different outcomes in different cases and appears to rest on the assumption that the same formula should apply under all circumstances. It remains to be seen whether the Advocate General and the Court will discuss the possible benefits of a more flexible approach or instead stick to an abstract assessment of the alternatives raised by the referred questions.

[51] Daphne Keller, 'The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation' forthcoming in Berkeley Technology Law Journal <https://law.stanford.edu/publications/the-right-tools-europes-intermediary-liability-laws-and-the-2016-general-data-protection-regulation/>.

[52] For an overview of some of these problems within the wider context of EU data protection law see Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23 MJ 812.

[53] Dan Svantesson, 'A 'Layered Approach' to the Extraterritoriality of Data Privacy Laws" (2013) 3 IDPL 278; Dan Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law 53, 67.

Spain ruling but arguably underlies EU data protection law more generally. On the one hand, calling for unrestrained global reach might on paper offer better protection of individual rights and support the EU's ambition to act as a global trendsetter in the field by stimulating spontaneous convergence towards its stricter regulatory standard – a sort of 'Brussels effect'[54] for privacy and data protection. Inherent risks of this approach would be its possible limited effectiveness outside the EU borders and adverse effects on transatlantic relations.[55] On the other hand, any alternative approach that could do justice-better to the complexities of individual cases would also make it harder for online operators and data subjects alike to cope with the intricacies of EU data protection law. It would thereby increase barriers to entry in online markets[56] and possibly wide the gap between the law in books and the law in action.[57]

Interestingly, both approaches are likely to contribute to a process of fragmentation of the Internet that has been ongoing further for quite some time. This process whereby, in the wake of *Yahoo!* and similar cases, the web has been increasingly 'carved up' into discrete legal spheres by the exercise of sovereign regulatory power.[58]

The alternative between global and territorially selective delisting points, however, to two different models of fragmentation. In the territorially selective model, geographic filtering allows global undertakings to offer online services across a number of jurisdictions and permits the coexistence of a plurality of divergent local laws each in its own territorial sphere. By contrast, claims for the global application of local data protection laws (or any other

---

[54] Anu Bradford, 'The Brussels Effect' (2012) 107 Northwestern University Law Review 1.

[55] On the possible measures that third countries could adopt as a reaction ('blocking legislation') see Dan Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law 53, 94-95.

[56] See Emmanouil Bougiakiotis, 'The Implementation of the Google Spain Ruling' (2016) 24 IJLIT 311, 319; David Stute, 'Privacy Almighty? Tge CJEU's Judgment in Google Spain SL v AEPD' (2015) 36 Michigan Journal of International Law 649, 676-677.

[57] On the gap between the expectations raised by EU data protection law and its actual prospects of enforcement see Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 IDPL 250, 251-253.

[58] Thomas Schultz, ''Carving up' the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799.

local laws) coupled with the threat of 'market destroying measures'[59] could potentially undermine the ability of companies to offer their services in different jurisdiction. Yet, that risk could arguably materialise only in the presence of much stronger policy divergences than the current different understandings of freedom of expression across the Atlantic. The actual impact of the scope of search engines' delisting obligations on tensions in transatlantic relations should therefore not be overestimated.

7. SELECTED LITERATURE

Bradford A, 'The Brussels Effect' (2012) 107 Northwestern University Law Review

Berman P S, 'The Globalization of Jurisdiction' (2002) 151 Pennsylvania Law Review

Bougiakiotis E, 'The Implementation of the Google Spain Ruling' (2016) 24 IJILT

Brkan M, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23 MJ

Brkan M, 'The Court of Justice of the EU, Privacy and Data Protection: Judge-made Law as a Leitmotiv in Fundamental Rights Protection' In Brkan M and Psychogiopoulou E, (eds) *Courts, Privacy and Data Protection in the Digital Environment* (10 et seq, Elgar, 2017)

CNIL orders Google to apply delisting on all domain names of the search engine' (12 June 2015) <https://www.cnil.fr/fr/node/15790>

CNIL 'Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre de Google' (decision of 10 March 2017) <https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu>

[59] Namely measures that could penalise a foreign party for failure to comply with the forum law. For this notion see Dan Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law 53, 98. As examples of market destroying measures the Author mentions the prohibition for the foreign party to trade in the forum jurisdiction, the unenforceability of credits within that same jurisdiction and the exclusion from government contracts.

Conseil d'Etat 'Google Inc., application No. 399922' (19 July 2017) <http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC>

Crespi S, 'Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati' (2015) Rivista italiana di diritto pubblico comunitario 819

De Hert P and Papakonstantinou V, 'Google Spain. Addressing Critiques and Misunderstandings One Year Later' (2015) 22 MJ

Falque-Pierrotin I, 'Pour un droit au déréférencement mondial' (29 December 2016) Le Monde

Fleischer P, 'Three years of striking the right (to be forgotten) balance' <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/>

Fleischer P, 'Adapting our approach to the European right to be forgotten' (*Google in Europe*, 15 May 2017) <https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig/>

Frantziou E, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review

Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006)

Hijmans H, 'Right to Have Links Re-moved. Evidence of Effective Data Protection' (2014) 21 MJ

Keller D, 'The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation' forthcoming in Berkeley Technology Law Journal, available at <https://law.stanford.edu/publications/the-right-tools-europes-intermediary-liability-laws-and-the-2016-general-data-protection-regulation/>

Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4 IDPL

Kropf J W, 'Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD). Case C-131/1' (2014) 108 AJIL

Kuner C, 'Google Spain in the EU and International Context' (2015) MJ

Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges' In Hess B and

Mariottini C (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Nomos, 2015)

Laprès D A, 'L'exorbitante affaire Yahoo' (2002) Journal de droit international

Laurie B, 'An Expert's Apology' (21 November 2000) <http://apache ssl.securehost.com/apology.html>

Lessig L and Resnick A, 'Zoning Speech on the Internet: A Legal and Technical Model' (1999) 98 Michigan Law Review

Lynskey O, 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78, 3 Modern Law Review

Manopoulos A, 'Raising 'Cyber-Borders': The Interaction Between Law and Technology' (2003) IJLIT

Maier B, 'How Has the Law At-tempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IJLIT

Muir Watt H, 'Yahoo! Cybercollision of Cultures: Who Regulates?' (2002-2003) 24 Michigan Journal of International Law

Reidenberg J, 'Yahoo and Democracy on the Internet' (2002) 42 Jurimetrics

Reimann M, 'Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage' (2002-2003) 24 Michigan Journal of International Law

Rees C and Heywood D, 'The 'right to be forgotten' or the 'principle that has been remembered'' (2014) 30 Computer Law and Security Review

Reidenberg J, 'Technology and Internet Jurisdiction' (2005) 153 University of Pennsylvania Law Review

Sartor G, 'Search Engines as Controllers. Inconvenient Implications of a Questionable Classification' (2014) 21 MJ

Schultz T, ''Carving up' the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL

Spiecker I, 'A New Framework for Information Markets: Google Spain' (2015) 52 CML Rev

Stute D, 'Privacy Almighty? Tge CJEU's Judgment in Google Spain SL v AEPD' (2015) 36 Michigan Journal of International Law.

Svantesson D, 'Limitless Border-less Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review

Svantesson D, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law

Svantesson D, 'A 'Layered Approach' to the Extraterritoriality of Data Privacy Laws" (2013) 3 IDPL

Tambou O, 'Le droit à l'oubli numérique' (2017) 606 Revue de l'Union européenne

Tribunal de Grande Instance de Paris, order of 22 May 2000, UEJF and Licra v Yahoo! Inc. and Yahoo! France

Van Alsenoy B and Koekkoek M 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to be Delisted'' (2015) 5 IDPL

Zekos G I, 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction' (2007) 15 IJLIT

Since the Snowden revelations, the adoption in May 2016 of the General Data Protection Regulation and several ground-breaking judgments of the Court of Justice of the European Union, data protection and privacy are high on the agenda of policymakers, industries and the legal research community.

Against this backdrop, *Data Protection and Privacy under Pressure* sheds light on key developments where individuals' rights to data protection and privacy are at stake. The book discusses the persistent transatlantic tensions around various EU-US data transfer mechanisms and EU jurisdiction claims over non-EU-based companies, both sparked by milestone court cases. Additionally, it scrutinises the expanding control or surveillance mechanisms and interconnection of databases in the areas of migration control, internal security and law enforcement, and oversight thereon. Finally, it explores current and future legal challenges related to big data and automated decision-making in the contexts of policing, pharmaceutics and advertising.

Gert Vermeulen is full professor of international and European criminal law and director of the Institute for International Research on Criminal Policy (IRCP) at Ghent University, and privacy commissioner at the Belgian DPA.

Eva Lievens is assistant professor of law and technology at Ghent University.

www.maklu.eu
isbn 978-90-466-0910-1