The 'Right to be Forgotten' Online within G20 Statutory Data Protection Frameworks

David Erdos and Krzysztof Garstka[1]

Abstract:

Although it is the EU's General Data Protection Regulation and the Google Spain judgment which has brought the concept of the 'right to be forgotten' online to the fore, this paper argues that its basic underpinnings are present in the great majority of G20 statutory frameworks. Whilst China, India, Saudi Arabia and the United States remain exceptional cases, fifteen out of nineteen (almost 80%) of G20 countries now have fully-fledged statutory data protection laws. By default, almost all of these laws empower individuals to challenge the continued dissemination of personal data not only when such data may be inaccurate but also on wider legitimacy grounds. Moreover, eleven of these countries have adopted statutory 'intermediary' shields which could help justify why certain online platforms may be required to respond to well-founded ex post challenges even if they lack most ex ante *duties here. Nevertheless, the precise scope of many data protection laws online remains opaque and the relationship between such laws and freedom of expression is often unsatisfactory. Despite this, it is argued that G20 countries and G20 Data Protection Authorities should strive to achieve proportionate and effective reconciliation between online freedom of expression and ex post data protection claims, both through careful application of existing law and ultimately through and under new legislative initiatives.*

1. Introduction

Claims for a 'right to be forgotten' online assumed a high-profile public profile within data protection when the European Commission decided to include this phraseology within the General Data Protection Regulation (GDPR) text, the draft of which was released in January 2012[2] and finally agreed by the EU institutions in April 2016.[3] This new wording was prompted by vast expansion in the publication of personal data online, symbolised most especially by the rise of social networking. Thus, by December 2011 "1.2 billion users worldwide – 82 percent of the world's Internet population over the age of 15 – logged on to social media sites, up from 6 percent in 2007".[4] Moreover, mass social networking was only one part of the explosive dissemination and spread of personal data within the Web 2.0 environment which also encompassed such platforms as blogs, micro-blogs and rating websites. Moreover, by default, much of this information has been made seamlessly and instantly available through the organising efforts of powerful internet search services such as Google. In 2014, this latter aspect was addressed by the Court of Justice of the European Union (CJEU) holding that

[1] This is a working paper of the Human Rights, Big Data and Technology Project (HRBDT) which is funded by the UK's Economic and Social Research Council (grant number ES/M010236/1). For further information on the HRBDT project as a whole please see https://hrbdt.ac.uk/.

[2] COM (2012) 11 final, art. 17.

[3] Regulation 2016/679, art. 17

[4] Van Dijck, Jose, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press 2013), 4.

individuals' had a qualified right to "be 'forgotten'"[5] from results emanating at least from any internet search on an individual's name. Interestingly, that judgement was made under the Data Protection Directive 95/46, an EU instrument that was in place for some two decades prior to the finalisation of the GDPR. Moreover, despite claims to the contrary, this legal holding can hardly be dismissed as anachronistic even to data protection as it has existed historically. To the contrary, at least within Europe, this regime had deliberately adopted *"broad"* definitions with a view to ensuring *"effective and complete protection"* of individuals.[6] Moreover, concerns regarding the spread and perpetuation of personal data of all kinds through online publication have been raised within a European data protection context since at least the early 1980s.[7]

Highlighting the broad roots of the 'right to be forgotten' concept within European data protection links also to a recognition of its wider interface with other key data protection frameworks. Thus, European data protection's first legal iteration in the Council of Europe's Data Protection Convention of 1981 was developed alongside the drafting of the Organisation for Economic Cooperation and Development (OECD) Privacy Guidelines of 1980.[8] Moreover, although data protection law was rare outside Europe in the 1980s and 1990s, the period from the 2000s has witnessed a vast increase in the number of countries considering such framework to be necessary. Indeed, at the start of 2019, Graham Greenleaf calculated that over 130 jurisdictions have adopted 'data privacy' laws of some sort.[9] A major catalyst for this development has been the vast increase in the breadth, depth and power of information processing consequent to the mass development of the internet. Thus, turning more specifically to online publication, jurisdictions outside Europe have in no way been insulated from the social networking and other Web 2.0 phenomena noted above. For much the same reason, the same period has also seen a variety of transnational organisations outside Europe adopt data protection instruments including Asia-Pacific Economic Cooperation (APEC), the Economic Community of West African States (ECOWAS) and the Association of Southeast Asian Nations (ASEAN). In 2017, we analysed these instruments, together with the OECD Privacy Principles and the Council of Europe Data Protection Convention, in relation to the 'right to be forgotten' online. In sum, we found that all these transnational frameworks other than that formulated by ASEAN lent a general support to such a right and even the ASEAN instrument did so as regards inaccurate or incomplete data.[10]

Whilst seeking to break new ground, our 2017 publication had a number of limitations. In the first place, it focused only on search engines. This was reflective of not only the special attention given to such actors in public debate but also the fact that the application of the right in this context has been especially controversial and "undoubtedly raise[s] some uniquely challenging interpretative

[5] C-131/12 *Google Spain* at [89].

[6] Ibid at [34].

[7] See e.g. "Preserving Data Protection in the New Media", *Transnational Data Report* (1983), p. 416; Seip, "The Individual in the Age of Telematics", *Transnational Data Report* (1984), pp. 362-4.

[8] See Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 14.

[9] Greenleaf, Graham, 'Global data privacy laws 2019: 132 national laws and many bills", *Privacy Law and Business International Report*, February 2019, 14. It should be noted, however, that Greenleaf's conceptualisation of 'data privacy laws' is broader than our definition of data protection law. For example, jurisdictions with laws principally restricted to the public sector (e.g. the United States) are characterised as having 'data privacy law' but would fall outside our notion of data protection legislation.

[10] Garstka Krzysztof and David Erdos, "Hiding in Plain Sight: Right to be Forgotten and Search Engines in the Context of International Data Protection Frameworks" in Luca Belli and Nicolas Zingales (eds.), *Platform Regulations: How Platforms Are Regulated and How They Regulate Us* (FGV Direito Rio, 2017).

conundrums within data protection".[11] A much more weighty limitation of our previous piece arose from the fact that, in contrast to many aspects of the GDPR, the transnational instruments existing outside of the EU are not generally self-executing and so do not have direct effect within the legal order of the countries that have endorsed them. Therefore, in order to determine whether individuals might legally claim an online 'right to be forgotten' under data protection in these wider group of jurisdictions, it is imperative to examine local statutory law.

The territorial reach of the 'right to be forgotten' has assumed a particular prominence as a result of Case C-507/17 *Google v CNIL*,[12] a referral to the Court of Justice which has arisen from the French Data Protection Authority's claim that at least European residents should be able to claim a worldwide 'right to be forgotten' remedy against global operators such as Google. In an opinion published in January 2019, Attorney-General Szpunar suggested that, at least in ordinary cases, such an extraterritorial result would be inappropriate.[13] However, whatever the outcome of these proceedings, the challenges arising from the explosive dissemination of personal data online are profoundly global. Moreover, the robust realisation of a 'right to be forgotten' online will certainly require transnational coordination. This article, therefore, provides an initial analysis of the statutory framework within a wider range of jurisdictions as this relates to the 'right to be forgotten' online.

The paper specifically focuses on data protection law within the G20. This grouping encompasses not only the EU as a transnational body but also nineteen leading countries within the world economy and society. Beginning with this admittedly bounded group is justified partly on grounds of practicality. However, it is also prompted by the growing involvement of the G20 in questions connected to digitisation. Thus, in 2017 the Germany Presidency established a G20 Taskforce on the Digital Economy and published a Roadmap in this area.[14] The following year the Argentinian Presidency established a G20 Repository of Digital Policies.[15] Most recently, in June 2019 the G20 issued a Ministerial Statement on Trade and Digital Economy which stressed both the benefits brought by digital developments and the need to "address challenges related to [*inter alia*] privacy [and] data protection".[16] Finally, and perhaps most significantly, the G20 countries exert a dominant influence within the global economy and society. In sum, they account for around 85% of the gross world product, at least three quarters of world trade and some two thirds of the world's population.[17]

This paper is structured into nine sections. Following this introduction, section two explores how we approached the admittedly rather ambiguous (and sometimes controversial) concept of the 'right to be forgotten'. Section three then elucidates the presence and basic scope of statutory data protection frameworks within the G20. Following on from this, the next two sections explore the extent to which these frameworks grant individuals an *ex post* right to challenge personal data processing on the grounds, firstly, of 'inaccuracy' and then on wider legitimacy criteria. Section six

[11] Ibid, p. 127.
[12] Case C-507/17 *Google v CNIL.*
[13] Szpunar did, however, add that he did "not exclude the possibility that there may be situations in which the interest of the European Union requires the application of the provisions of [Data Protection] Directive 95/46 beyond the territory of the European Union" (at [62]).
[14] Germany, Bundesministerum für Wirtschaft und Energie, *G20 – shaping digitisation at the global level* (n.d.), https://www.de.digital/DIGITAL/Redaktion/EN/Dossier/g20-shaping-digitalisation-at-global-level.html (NOTE: all links cited in this paper were accessed on 9 September 2019).
[15] G20 Ministerial Statement on Trade and Digital Economy (2019) at [8], https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf .
[16] Ibid at [16].
[17] European Parliament, *The Group of Twenty (G20) Setting the global agenda* (2015), http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/545712/EPRS_BRI(2015)545712_REV1_EN.pdf.

then considers the general tension between our qualified conceptualisation of the 'right to forgotten' and the widespread presence within the G20 of apparently peremptory substantive default rules especially as regards 'sensitive' data. Section seven then analyses countervailing substantive limitations within these frameworks designed to safeguard freedom of expression, whilst section eight explores statutory 'intermediary' liability shields which could help justify why various online platforms such as search engines might be absolved from most *ex ante* duties whilst still being required to respond to 'right to be forgotten' demands *ex post*. The final concluding section provides a summary and discussion of the paper's findings. Drawing on this, it also suggests a way for the G20 and the G20's Data Protection Authorities to confront these new 'right to be forgotten' challenges.

2. Delimiting the 'Right to be Forgotten' Online

The 'right to be forgotten' is far from an uncontested or unambiguous term. In light of this, it is important to spend some time at the outset exploring its meaning. To the best of our knowledge, only one legal instrument – namely the EU's GDPR – explicitly grants individuals something which it explicitly labels a 'right to be forgotten'.[18] Seen from a highly formal perspective, therefore, it could be argued that only EU law recognises this concept. Such a perspective, however, would not only be trite but also highly misleading. To begin with, the place of the 'right to be forgotten' within EU law itself is highly complex. Even before the GDPR was enacted, it had been explicitly recognised by the Court of Justice of the EU (CJEU) in its *Google Spain* decision of 2014, which specifically held that individual data subjects should have a presumptive ability under data protection to mandate that search engines deindex personal data relating to them. That seminal holding was grounded in three explicit rights within the then extant EU data protection scheme, namely, the right to have personal data rectified where it was inaccurate,[19] the right otherwise to have illegally processed data erased[20] and the right to object to processing on compelling personal grounds.[21] The GDPR as agreed in 2016 carries forward all of these rights, whilst adding the term 'right to be forgotten' in brackets alongside one of these, namely, the right to erasure.[22] The 'right to be forgotten' within the GDPR is, therefore, not clearly distinguished from any of these other control rights and, moreover, is especially fused to the pre-existing right of erasure.[23]

All the aforementioned legislative and judicial elements encapsulate a common focus on ensuring that individuals are able to use data protection law, including in an online context, in order restrict access or otherwise exercise control over information identifying (with a view to preventing actual or potential harm), provided that there are no overriding, legitimate reasons to oppose such restriction or control. This broad understanding of the online 'right to be forgotten' will, therefore, be the one deployed in this article.

[18] GDPR, art. 17 (though the brackets around this term indicate the controversy it raises)
[19] Data Protection Directive 95/46, art. 12(b).
[20] Ibid, art. 12(b).
[21] Ibid, art. 14.
[22] GDPR, arts. 16 (right to rectification), 17 (right to erasure) and 21 (right to object).
[23] Indeed, the only clearly new 'right to be forgotten' element added to the GDPR text is a stipulation requiring that those controllers who are subject to a *bona fide* right to erasure and who have made that data public "take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data" (Ibid, art. 17(2)).

A new focus on the use of these *ex post* data protection remedies in an online context has undoubtedly been catalysed by the explosive growth in both the range and quantity of personal data being published and processed online over recent years. This began with development of both blogs[24] and internet search engines[25] in the early 2000s and reached a new crescendo as a result of the rise of social networking sites from the latter 2000s onwards.[26] It has, however, been erroneously claimed that the CJEU essentially spawned approach *de novo* in *Google Spain* and, relatedly, that the 'right to be forotten' was and is uniquely focused on search engines. For example, Byrum (2018) claims that that the "European Right to be Forgotten" is "a legal construct that was recognized by the European Union in 2014, allowing individual Europeans the opportunity to petition search engines for the removal of data that is deemed inaccurate or no longer relevant",[27] whilst Kaye similarly states that "*Google Spain*, as the case that gave birth to the 'right to be forgotten' is known, provides Europeans with a right to ask a search engine like Google to delink or de-index a website from the name-based search results if it meets the conditions of irrelevance".[28] In fact, this concept is not only much broader but also has deep roots within data protection, at least as it has emerged in Europe. Thus, as early as 1984, the head of the Norwegian Data Protection Authority argued that a critical question for data protection to address was "to what extent it is possible to give persons fair and necessary access to what personal information is reported about them through the data banks of press information, and how far is there a chance that wrong and misleading information could be corrected and adjusted in ways that prevent harm occurring".[29] Meanwhile, in 2001 a *déliberation* from the French DPA argued that given contemporary online realities (including, most notably, the growing sophistication of search engines) the *"droit à l'oubli"* pointed to the need in most circumstances for jurisprudential information to be anonymized prior to its publication online.[30] Although tantalizing, this article will not examine further the development of the 'right to be forgotten' over time, or its various identified forms – which has already been the subject of valuable study by Voss and Castets-Renard (2016).[31] Rather, it will seek to explore the related and even more critical question of whether this concept has a broad geographical reach, potentially stretching far beyond the EU. Crucially, this requires an analysis of the various ways in which the 'right to be forgotten' idea might be considered embedded within fundamental concepts which exist in many legislative data protection frameworks not only within Europe but also further afield.

A number of commentaries on the 'right to be forgotten' including in particular, in the United States have emphasised its tension with freedom of expression. Most notably, Jeffrey Rosen (2012) criticised the (initial draft of the) GDPR for creating "a sweeping new privacy right – the 'right to be

[24] Solove, Daniel, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* (Yale University Press, 2007), p. 21.
[25] Ibid, p. 9.
[26] Jose Van Dijck, *The Culture of Connectivity* (2013), p. 4.
[27] Byrum, Kristie, *The European Right to be Forgotten: The First Amendment Enemy* (Lexington Books, 2018), p. 147.
[28] Kaye, David, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports, 2019), p. 34
[29] Seip, Helge, "The Individual in the Age of Telematics", *Transnational Data Report* (1984), 363.
[30] France, Commission nationale de l'informatique et des libertés, *Délibération n° 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence*, https://web.archive.org/web/20130614052958/https:/www.cnil.fr/documentation/deliberations/deliberation/delib/17/.
[31] Voss, W. Gregory and Céline Castets-Renard, 'Proposal for an International Taxonomy on the Various Forms of the "Right to be Forgotten": A Study of the Convergence of Norms', Colorado Technology Law Journal (Vol. 14(2), pp. 281-343) (2017).

forgotten'", arguing that "it represents the biggest threat to free speech on the Internet in the coming decade".[32] As previously noted, the idea that the GDPR's reforms here represented something conceptually novel is simply incorrect. On the other hand, the need to reconcile the 'right to be forgotten' with freedom of expression is very real. In that context, it is critical to stress that the 'right to be forgotten' must not be understood as an absolute right; to the contrary, the imperative to balance it with freedom of expression falls out of our understanding that it should be superseded by genuine 'overriding, legitimate reasons' for the continuing processing of data. Albeit highly imperfectly, this need is also recognised in a number of provisions in the GDPR itself including the requirement that Member States legislate wide-ranging limitations on data protection in relation to journalism as well as academic, artistic and literary expression,[33] a broader (but much more cryptic) requirement to reconcile data protection with freedom of expression generally[34] and a disabling of the right to erasure "to the extent that processing is necessary for exercising the right to freedom of expression and information".[35] Meanwhile, although the CJEU should have been explicit on this point, this need was also implicitly recognised in the *Google Spain* judgment, both when restricting the circumstances when search engines would need to act[36] and when holding that processing could continue when "justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question".[37] The CJEU will shortly reconsider these issues in the context of both the geographical reach of a search engine's deindexing obligations under *Google Spain*[38] and the interface between this holding and the GDPR's sensitive data and accuracy provisions. In this context, it is striking that the Advocate General Opinion in the latter case begins by noting that "[r]econciling the right to privacy and to the protection of personal data with the right to information and to freedom of expression in the internet era is one of the main challenges of our time".[39] In sum, therefore, the need for a balanced relationship with freedom of expression should be seen as an integral part of the 'right to be forgotten' concept properly conceived rather than being (as Rosen suggests) intrinsically antagonistic to it. This admittedly very tricky issue will be returned to at various points in this article including, in particular, sections six to eight. Before doing so, however, we turn to the core issue of the article, namely, to what extent the 'right to be forgotten' concept is in principle recognised within the data protection frameworks found in G20 countries.

3. Statutory data protection frameworks in the G20

Our search for the presence of the 'right to be forgotten' in G20 legislative frameworks commenced with a survey of whether, and to what extent, these jurisdictions had adopted data protection legislation that extended to the disclosure and further use of personal data online. To this end, we formulated two questions: firstly, whether the studied jurisdictions contained data protection

[32] Rosen, Jeffrey, "The Right to be Forgotten", *Stanford Law Review Online* (Vol. 64, pp. 88-92) (2012).
[33] GDPR, art. 85(2).
[34] Ibid, art. 85(1).
[35] Ibid, art. 17(3)(a).
[36] In sum, the Court found that a search engine would only have substantive duties here where its activity was "liable to affect" data subjects' rights "significant, and additionally compared with that of the publishers of websites" and even the only needed to act "within the framework of its responsibilities, powers and capabilities" (C-131/12 *Google Spain* at [38]).
[37] Ibid at [97].
[38] C-507/17 *Google v Commission nationale de l'informatique et des libertés*.
[39] C-136/17 G.C., A. F., B. H.,E.D. v *Commission nationale de l'informatique et des libertés* (Advocate General Opinion), EU:C:2019:14 at [1].

legislation at all and, secondly, amongst the countries which did, what limitations applied which could generally exclude the applicability of the law to processing involving the online disclosure of personal data.

As in the entirety of our analysis, we drew on legislative material which had been published online. These are set out in the two appendices of this article. As can be seen in appendix one, in almost all cases we were able to source English language versions of the relevant data protection statutes. These texts had been produced by the legislature itself (e.g. in Australia, the EU and South Africa), by an official government agency (e.g. in Argentina) or by a reputable private entity (e.g. the principal Russian data protection law). In a few cases, however, data protection legislation could only be located in a non-English original language version. As is apparent in appendix two, this was also the case in relation to a few of the statutory intermediary shield laws examined in section eight. In all these cases, which are highlighted in italics within the two appendices, we drew on our own translation of the relevant legislation.

3.1 – Existence of data protection legislation

For the purposes of this paper, data protection law was conceptualised as a relatively comprehensive statutory code that governs the use or processing of information which is about or relates to an identifiable and specific natural person. In total, we found that fifteen out of the nineteen G20 countries, as well as the EU as a whole, clearly had such a law. These jurisdictions fell within this rubric even if their legislation styled itself using divergent terminology or, whilst on the statute book, had yet to come into force. For example, the relevant Australian law legislation was badged as a "Privacy Act" rather than a data protection act. Meanwhile, the Brazilian General Data Protection Law was adopted in 2018 but will not become operational until the first half of 2020.[40] The substantive provisions in the South African Act are similarly not expected to come into force until 2020.[41] Finally, Russia had enacted not only an omnibus data protection law but also one specifically focused on establishing the circumstances under which individuals could require search engines to deindex personal data.

The four 'outlier' cases were China, India, Saudi Arabia and the United States. However, notwithstanding this commonality, it is important to draw certain distinctions *within* this group. Thus, Saudi Arabia does not have any law resembling data protection and the United States has generally only legislated on specific matters within particular social or economic sectors.[42] Meanwhile, in 2016

[40] General Data Protection Law 2018, art. 65.

[41] See Frank Madden, "South Africa's POPIA expected to enter into force in 2010", 160 (2019) *Privacy Laws and Business International Report* 26.

[42] For example, aside from the public sector (which is regulated under the Privacy Act 1974), legislation is restricted to specific issues and areas such as the Health Information Portability and Accountability Act from 1996 (regulating the use of people's medical data), the Children's Online Privacy Protection Act from 1998 (dealing with children's personal information) and the Gramm-Leach-Bliley Act from 1999 (focused on financial institutions and their information-sharing practices). Some State laws do go further including, in particular, the California Consumer Privacy Act (2018) which from 1 January 2020 will regulate a wide variety of personal information usage or processing of businesses which operate in that State. However, this law is restricted to businesses which reach $25 million in annual revenue, trade in personal information tied to at least 50,000 individuals, households or devices and/or derive at least 50% of their annual income from selling personal data. Even more pertinently for our purposes, this law is largely limited to transparency-related obligations and excludes a wide range of "publicly available information".

China did adopt a cybersecurity law which *inter alia* obliged "network operators" to abide by "the principles of legality, propriety and necessity" when collecting and using personal information and publish "rules for collection and use, explicitly stating the purposes, means and scope for collecting or using information, and obtain the consent of the persons whose data is gathered".[43] The meaning of 'network operators' remained rather opaque but seems essentially focused on back-end processing operators rather than publication-related activities which are the focus of this article. This law also imposed a generally applicable duty of lawfulness in the acquisition, selling or provision of personal information. However, it failed to specify what precise standards attached to this requirement of legality.[44] Moreover, all these legal provisions must be placed against the "complex surveillance system touching all aspects of Chinese society" which underpins the "political control of the Communist Party" in that country.[45] Finally, Indian law does set out certain limited information rules which are applicable (only) to certain categorically defined 'sensitive' classes of personal information.[46] Even more restrictively, these rules are rendered entirely inapplicable to "information that is freely available or accessible in the public domain".[47] The latter types of information are clearly central to this paper. Therefore, all four of these countries fail to meet the threshold for data protection law as we have approached this. Nevertheless, it should be acknowledged that both China and India do have extensive statutory provisions which are widely applicable to the private sector and are often treated in other contexts as 'data privacy laws'.[48]

3.2. General Limitations Within Data Protection Laws

Even when confining our attention to the fifteen G20 countries with relatively comprehensive laws, all these frameworks contained certain generally formulated limitations that potentially excluded the applicability of data protection to some or all online publication-related activity. In the first place, the data laws in eleven of these countries[49] contained some kind of exemption for natural persons when pursuing personal or household activities. However, whilst it is undoubtedly true that amateur individuals are directly responsible for the online publication of a wide range of personal data concerning third parties, it cannot be assumed that this exemption will generally shield them from all scrutiny under data protection. To the contrary, this personal exemption has generally been worded restrictively even outside of the EU. For example, the omnibus Russian data protection law requires that any such processing "does not infringe the rights of personal data subjects".[50] Furthermore, in a number of cases, the exemption is explicitly disabled in cases where data is published. Thus, the Turkish law requires that such data are "not transferred to third parties",[51] whilst the Mexican

[43] China, Cybersecurity Law, Art. 41.
[44] Ibid, art. 44.
[45] Greenleaf, Graham, *Asian Data Privacy Laws* (Oxford University Press, 2014), p. 195.
[46] India, Privacy Rules, sec. 3. For further discussion of the concept of 'sensitive' data see section six.
[47] Ibid, sec. 3.
[48] See, for example, Greenleaf (2019), supra note 9.
[49] Namely, all four EU countries with the G20 (GDPR, art. 2(2)(c)), Australia (Privacy Act 1988, sec. 16), Brazil (General Data Protection Law, art. 4(I)), Canada (Personal Information Protection and Electronic Documents Act, s. 4(2)(b)), Mexico (Federal Law on the Protection of Personal Data held by Private Parties, art. 2.ii), Russia (Data Protection Act No. 152 FZ, art. 1(2)(1)), Turkey (Law 6698 on the Protection of Personal Data, art. 28(1)(a)) and South Africa (Protection of Personal Information Act, No 4 of 2013, art. 6(1)(a)).
[50] Russia, Data Protection Act No. 152 FZ, art. 6(2)(6).
[51] Turkey, Law 6698 on the Protection of Personal Data, art. 28(1)(a).

excludes any processing for the "purposes of disclosure".[52] In any case, data posted online by natural persons may increasingly come under the effective 'control' of online platforms of various sorts. In such instances, these legal entities may themselves acquire obligations either under the omnibus data protection legislation or, in the case of Russia, additionally under its *sui generis* data protection law regulating search engine indexing.[53]

A second group of three countries (Canada,[54] Japan[55] and Korea[56]) went further by entirely excluding processing by natural or legal persons outside who, outside of the public sector, are pursuing non-commercial purposes.[57] The Australian legal framework was somewhat similar. The personal exemption here explicitly extended to the "disclosure of personal information by an individual" so long as this remained at least "in connection with, his or her personal, family or household affairs".[58] The law also set out an exclusion for small businesses,[59] which were generally defined as those having a turnover of less than AU$3 million.[60] However, although undoubtedly extensive, none of these exemptions in any of these four countries necessarily shielded the activities of the large commercial online platforms which often exercise significant control over published personal data in today's digital environment.

Third and finally, many G20 laws either only extended their data protection laws to the electronic use or manipulation of personal data or, in the case of manual data, required the information to be systematically organised. Given that the subject matter of this paper is entirely 'online', these restrictions have no real impact on our area of focus. In contrast, however, the laws of four countries (Argentina, Indonesia, Japan and Korea) appeared to require that even electronically manipulated data be organised in some way before they fell within data protection controls.[61] Thus, Argentinian law only applied to an "organized set of personal data which is subject to treatment or processing", Indonesian law talked of the "organizer of the Electronic System",[62] Japanese laws referenced a "collective body of information" which is "systematically organized so as to be able to search for particular personal information using a computer"[63] and Korean law only covered "a set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy access to the information".[64] It is not easy to determine to what extent these limitations might restrict the application of the law vis-à-vis processing connected to the dissemination of personal data online. Arguably, any data published on the open internet will likely become systematically organised

[52] Mexico, Federal Law on the Protection of Personal Data held by Private Parties, art. 2.ii.
[53] Federal Law of 13.07.2015 N 264-FZ "On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection'"
[54] Canada, Personal Information Protection and Electronic Documents Act, s. 4(2)(b).
[55] Japan, Act on the Protection of Personal Information 2005, art. 5 (referring only to "business operators").
[56] Korea, Personal Information Protection Act 2011, s. 2(5) (referring only to operators engaging in "official or business purposes").
[57] The limited Indian rules concerning non-public 'sensitive' data discussed in section 3.1 above were similarly only applicable to those "engaged in commercial or professional activities" (India, Privacy Rules 2011, sec. 2(c) (referencing definition in Indian Information Technology Act, s. 43A)).
[58] Australia, Privacy Act 1988 (as amended), sec. 16.
[59] Ibid, sec. 6c.
[60] Ibid, sec. 6d.
[61] Somewhat similarly, the laws in Argentina and Mexico reserved some (but not all) data protection duties to such systematically organised material. See Personal Data Protection Act 25.326, section 2 (Argentina) and Federal Law on the Protection of Personal Data held by Private Parties, art.3(II) (Mexico).
[62] Indonesia, Data Protection Regulation, art. 1(6).
[63] Japan, Act on the Protection of Personal Information, art. 2(4).
[64] Korea, Personal Information Protection Act 2011, art. 2(2).

since, whereas information published in traditional formats is "hard to retrieve, and a sleuth would have to devote a lot of time to dig it up", information on the internet "can be readily found in less than a second"[65] as a result of electronic search facilities of various sorts. In any case, it is clear that as online platforms engage in the ever more advanced promotion, aggregation, arrangement and pushing of data, the potential for data to be considered to be systematically organized will continue to increase. As it does then data protection law will tend to bite even within this last subgroup of countries.

4. Rights in relation to Inaccuracy

It makes sense to commence our substantive analysis of the 'right to be forgotten' online by looking at issues relating to data inaccuracy. The substantive idea that individuals should be able to ensure the rectification of significantly inaccurate data has generally been seen as both more discrete and less controversial than the claim that the legitimacy of the processing any personal data may be similarly challenged. Not only does such an ability have a strong affinity with long-standing standards set down in defamation law,[66] but our earlier analysis of transnational data protection found that this aspect was the only one found in all of the international frameworks under study.[67] More specific to the focus of this paper, much of the backlash to the *Google Spain* judgment deliberately excluded criticising this holding as it pertained specifically to inaccurate data. This is apparent, for example, in the UK House of Lords EU Committee's (in any case unsuccessful) call for a reform to EU law "which does away with any right allowing a data subject to remove links to information *which is accurate* and lawfully available"[68] but made no such demand as regards as regards inaccurate information. Similarly to the examination of general legitimacy below, our analysis here is divided into two parts. To begin with, we explored whether and how data subjects were provided with an explicit *ex post* right to challenge inaccuracy. Following this, we also sought to locate underlying substantive standards in the law that either supported any explicitly enunciated right or even potentially impliedly created such a right itself in circumstances where these standards had been breached.

Beginning with the headline results, we found that *ex post* rectification rights were present in all fifteen G20 countries with a data protection law. We also found that all of these laws also set out substantive standards that ungirded this right.[69]

---

[65] Solove, Daniel, *The Future of Reputation* (Yale, 2007), p. 33.

[66] Thus, at least traditionally, defamation law has generally sanctioned the publication of any untruthful (or inaccurate) claim which impacts on the reputation of an individual. Moreover, at least in the UK, it has even been held that it is for the publisher to prove the truthfulness or accuracy of any reputation-impacting statement. See David Erdos 'Data Protection and the Right to Reputation' 73 (2014) Cambridge Law Journal 536 at 539-41 and also Krzysztof Garstka 'From Cyberpunk to Regulation: Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law' 8 (2017) JIPITEC 293, at 299.

[67] Garstka and Erdos, "Hiding in Plain Sight: Right to be Forgotten and Search Engines in the Context of International Data Protection Frameworks" (see fn. 10), p. 144

[68] UK, House of Lords, European Union Committee, *EU Data Protection law: a 'right to be forgotten'?* (2014), p. 22 (emphasis added), https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf

[69] Within the narrow confines within which it operated, the data privacy rules in India similarly empowered data subjects to challenge inaccuracy *ex post* but did not include any wider principles which directly related to this. See Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules 2011), rule 5(6).

Our deeper analysis revealed interesting patterns related both to the substantive and remedial provisions of the law here. In the first place, it was clear that the concept of 'accuracy' was generally construed broadly. Thus, almost all the laws examined sought not only to control data which was inaccurate *sensu stricto* (i.e. manifestly false) but also that which was incomplete or was not up-to-date. In a few cases, further explicit augmentations were present. For example, the Argentinian standards were explicitly made applicable not only to "totally" but also "partially" inaccurate data,[70] whilst Australian law enabled data subjects to challenge merely "misleading" data.[71] The conceptualisation of accuracy set out in the *ex post* right and the underlying data standard were usually, but not always, identical.[72] Finally, in certain cases, conformity with some of these standards was expressly made conditional on it being necessary given the context or the purpose of the processing at issue. This was especially apparent as regards the notion that data should be up-to-date or timely, a requirement which is manifestly apposite in some situations (e.g. a website seeking to keep track of a professional's current skills and qualifications) but not others (e.g. a website clearly concerned with recording historical data).

Turning finally to the remedial aspect, in most cases the law focused entirely on the notion that data should be corrected. However, in a few countries, this remedy was fused to other possibilities, such as that there might be a "deletion" of data or the "addition" of new data (e.g. in Canada[73] and Japan[74]). These broader possibilities generally arose in a context where remedies were listed in bulk next to a wide variety of potential challenges to processing only some of which related to inaccuracy. Nevertheless, once the broader meaning of accuracy is taken into account, it is clear that remedies such as adding data will sometimes be appropriate, notably when the claim is not that data is directly false but that it needs to be completed. In Canada, this contextual aspect was explicitly captured by a stipulation that the remedy provided should depend on "the nature of the information [being] challenged".[75]

5. Rights relating to the General Legitimacy of Processing

Enabling processing to be objected to on the basis of a lack of completeness and/or timeliness in data naturally segues into a wider claim that individuals should be able to challenge the legitimacy of processing even entirely accurate data so long as their rights and interests outweigh the rights and interests in the continued processing. To take a concrete example, whilst the previous analysis could cover a situation where an individual objects to a social media post which incorrectly labels him as guilty of fare dodging or even one which fails to specify the length of time which has elapsed since any such infraction, this section examines whether this individual could restrict such a post on the basis,

[70] Personal Data Protection Act 2000 25/326, s. 4(5).
[71] Australian Privacy Principles, principle 13.
[72] A particularly large gap was apparent in the case of the general data protection law in Russia. Here, the basic data principle required that personal data conform to "reliability" (Federal Personal Data Law No. 152 FZ, art. 5(1)(4)), a rather elliptical standard which nevertheless clearly related to the core notion of accuracy. In contrast, the ex post right clearly enabled the data subject to control data processing which was "incomplete" or "outdated" (Personal Data Law, art. 14(1)) but did not explicitly empower him or her to require action in relation to data which was simply false.
[73] Personal Information Protection and Electronic Documents Act, para. 4.9.5. of Schedule 1.
[74] Act on the Protection of Personal Information 2005, art. 29.
[75] Personal Information Protection and Electronic Documents Act, para. 4.9.5. of Schedule 1.

for example, of a right to rehabilitation even when the information published was neither false nor misleading.

As with accuracy above, we looked both for the presence of a relevant *ex post* right and for substantive data principles or standards which related to the general legitimacy of processing. Turning to the expressly remedial aspect first, we found that fourteen of the fifteen G20 countries with data protection law did explicitly enable individuals to challenge processing which might lack this wider type form of legitimacy. The only complete exception here was Canada, although Turkey did exclude this right in any case where the data in question had been manifestly made public by the data subject themselves.[76] In most cases it was clear that such a right could in principle result in complete erasure or deletion or data (e.g. Korea[77] or Brazil[78]). However, in a few countries the law spoke only of a somewhat lesser remedy such as requiring that the controller "supress or keep [the data] confidential".[79]

Turning to the substantive notion of legitimacy embedded in the legislation, in many countries the law clearly enabled data subjects to mount a challenge on the grounds that processing was excessive and/or lacked proportionality (e.g. not only G20 EU countries[80] but also Argentina, Brazil, Korea, and Russia). For example, Argentina stipulated that personal data must "not [be] excessive with reference to the scope and purpose for which such data were secured",[81] Brazil that data must be "proportional and non-excessive in relation to the purposes of the data processing",[82] Korea that processing "minimize the possibility to infringe the privacy of [the] data subject"[83] and Russia that data not be "excessive relative to the purposes stated during personal data gathering".[84] In contrast, aside from the special case of sensitive data which is examined further in the next section, the general standards enunciated in some other laws were either more opaque or less exacting. For example, Australian law only generally sought to restrict data that was not "relevant" to the processing purposes,[85] Indonesian law similarly restricted processing not "in accordance with the provisions of laws and regulations"[86] and finally Japan restricted processing which went beyond that which was "necessary" to achieve the processing purpose.[87]

Turning finally to the special case of Canada, although no explicit and generally applicable *ex post* right was set down here, the law did state that "[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate".[88] Where a data subject brings an example of processing which is having a clearly disproportionate impact on them to the attention of a controller then the continued processing of

[76] Data Protection Law 2016, art. 28(2)(b).
[77] Personal Information Protection Act 2011, art. 4(4).
[78] General Data Protection Law 2018, art. 18(IV).
[79] See Argentina: Personal Data Protection Act 2000 25/326, s. 16(1).
[80] GDPR, art. 17(1)(d) (enabling a challenge on the basis that the processing lacks conformity with any other aspect of the law, including for example that the core data protection principles (art. 5) are contradicted) and art 21(1) (enabling a challenge on any grounds relating to individual's particular situation which can only be defeated where the controller "demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishing, exercise or defence of legal claims").
[81] Personal Data Protection Act 2000 25/326, 4(1).
[82] General Data Protection Law 2018, art. 6(III).
[83] Personal Information Protection Act 2011, s. 3(6).
[84] Data Protection Act 2006, art. 5(4).
[85] Australia, Privacy Act, Sch. 1 (Australian Privacy Principles), principle 10.2.
[86] Data Protection Regulation 2016, s. 9(1).
[87] Act on the Protection of Personal Information 2005, art. 16(1).
[88] Personal Information Protection and Electronic Documents Act, s. 4(3).

such data absent their consent would almost certainly become inappropriate. A clear example here might be an intimate image published without consent as 'revenge pornography'. Therefore, even in Canada, data subjects would appear to be granted some ability to challenge the legitimacy of processing beyond situations where a narrow or even a broad conceptualisation of inaccuracy is said to be infringed.

6. Principles, Rules and Sensitive Data

As previously emphasised, our understanding of the 'right to be forgotten' online conceptualises this as a qualified right which can be limited or even extinguished when there are compelling legitimate reasons justifying the continued dissemination of personal data. In principle, such a right must be supported by relatively flexible substantive norms that can be interpreted contextually. The standards discussed above broadly comport to such a mould or structure. This is most clear in relation to non-excessiveness or proportionality principles which clearly require the lawful interests of the controller to be balanced with the rights and interests of the data subject. However, even more apparently absolute principles incorporate a significant amount of definitional flexibility. For example, what might be considered an "adequate" presentation of the details of, say, a third party's public financial dealings when made within the context of an informal online discussion may not be so within an official report. Admittedly, the concept of "accuracy" can appear rather more peremptory. However, as section three highlighted, some laws incorporate important shades of meaning here, recognising that data may range from positing manifest untruths to being seen (depending on context) as incomplete or misleading. It is also significant that there is widespread agreement that the core of the principle of accuracy is relevant to the handling of information about individuals in a wide range of publication contexts including even in the particularly delicate area of journalism. For example, Lord Justice Leveson's report on the UK Press found that it was "not by accident that the Editors' Code begins with a requirement for accuracy", arguing that this was "the foundation stone on which journalism depends".[89] Nevertheless, tensions certainly remain. Thus, Leveson went on to note that "[i]t is important to note that it is inevitable that inaccuracies will appear in newspapers, given the quantity of stories published and the speed at which they need to be written".[90] Certainly, much the same could be said of a whole range of online publications, especially on social media. It would appear clearly disproportionate to mandate that even very minor inaccuracies online be amended at source or, in the case of a search result, be deindexed. Indeed, this is recognised in the aforementioned UK Editors' Code which only states that a "significant" inaccuracy should be "corrected, promptly and with due prominence".[91] However, such explicit nuance was almost invariably found to be absent in the default accuracy standards set down within the G20 data protection frameworks.

An even greater lack of nuance and flexibility was found to be present in most of the G20 data protection frameworks when processing involved what was defined as 'sensitive' data. Aside from Indonesia, all fifteen G20 countries with data protection statutes recognised a concept of 'sensitive' data within their law. Moreover, with the exception of Canada,[92] this concept was defined by

[89] Leveson, Brian, *Inquiry into the Culture, Practices and Ethics of the Press* (HC 2012, 780 I), 673.
[90] Ibid, 674.
[91] Independent Press Standards Organisation, *Editors' Code of Practice*, section 1(ii), https://www.ipso.co.uk/editors-code-of-practice/ (accessed 25 July 2019).
[92] Canadian law was much more open (and opaque) in its definition of sensitive information, although it did state that information such as "medical records and income records" is "almost always considered to be sensitive" (Personal Information Protection and Electronic Documents Act, art. 4(3)(5))

reference to wide categories of data that were deemed to raise heightened privacy or discrimination risks for data subjects. Commonly such categories at least encompassed data concerning health, sex life, race, religious or similar beliefs and political opinions.[93] Again with the exception of Canada[94] and potentially also Russia[95] and Mexico,[96] the collection or processing of such data was generally prohibited absent either waiver from the data subject[97] or a pre-identified exceptional circumstance arising. The circumstances specified were almost invariably specific and casuistic. Examples include where the processing was necessary for legal claims or the effectuation of justice (e.g. G20 EU countries,[98] Russia[99]), to protect the vital interests of the data subject or another person (e.g. G20 EU countries,[100] Russia[101]) or for reasons of health or hygiene (e.g. Australia,[102] G20 EU countries,[103] Turkey,[104] Japan[105]). Admittedly, in a few cases, these kind of specific clauses were combined with broader (but more opaque) provisions which permitted processing where other "laws" required or authorized this (e.g. Australia,[106] Korea[107]). However, even these provisions arguably continued only to legitimate data processing in exceptional and limited situations, as opposed to setting down substantive standards which enabled such processing in a wide and indeterminate (but not unlimited) set of circumstances. Turning back to Indonesia, although lacking a concept of sensitive data, the law here required that the acquisition or dissemination of any type of personal data by an "Electronic

[93] Brazilian law did, however, add as a caveat that its sensitive data rules should only apply when processing "may cause harm to the data subject" (General Data Protection Law 2018, art. 11(1)).

[94] Canadian law merely stated that "[a]n organisation should *generally* seek express consent when the information is likely to be considered sensitive" (Personal Information Protection and Electronic Documents Act (PIPEDA), s. 4.3.6) (emphasis added). Otherwise, such data remained governed by the general requirement that ""[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, *except where inappropriate*" (PIPEDA, s. 4(3)) (emphasis added).

[95] In Russia a peremptory sensitive data scheme as discussed below did generally apply but this was made inapplicable where "the personal data are public" (Federal Personal Data Law, art. 10(2)(2)). In the context of our paper, this latter exemption arguably results in even this most sensitive data which has been posted online being governed only by the general standards set out within the law.

[96] Mexican law generally required consent to obtained in order to legitimise the processing of any (and not just sensitive) personal data (Federal Law on the Protection of Personal Data held by Private Parties, art. 8). However, this requirement was lifted in various circumstances as set out in article 10 including (as is most relevant to this paper) where "[t]he data is contained in publicly available sources" (Ibid, art. 10(II)). Another provision stated that where sensitive data was processed then express written consent had to be obtained (Ibid, art. 9). It remained slightly ambiguous whether the article 9 stipulations were also intended to be lifted in all the circumstances set out in article 10.

[97] Waiver was almost understood to require the positive consent (and sometimes even the written consent) of the data subject. However, in the EU G20 countries it is also applied where data was being manifestly made public by the data subject (GDPR, art. 9(2)(e)) and in South Africa where the "information has deliberately been made public by the data subject" (Protection of Personal Information Act, No 4 of 2013, art. 27(1)(e)).

[98] GDPR, art. 9(2)(f).

[99] Data Protection Act 2006, art. 10(2)(6).

[100] GDPR, art. 9(2)(c).

[101] Data Protection Act 2006, art. 10(2)(3).

[102] Privacy Act, Sch. 1 (Australian Privacy Principles), principle 3(4)(c).

[103] GDPR, art. 9(2)(h).

[104] Data Protection Law, art. 6(3).

[105] Act on the Protection of Personal Information 2005, art. 17(2)(iii).

[106] Privacy Act, Sch. 1 (Australian Privacy Principles), principle 3(4)(a).

[107] Personal Information Protection Act 2011, art. 23(1)(2).

System Provider" needed to be based either on consent or on a provision in another law or regulation.[108] Therefore, this approach merely generalised the inflexibilities identified in this section.

Seen from the perspective of the data subject, the presence of binding and inflexible rules may greatly strengthen the value of data protection within the online environment. Certainly, these provisions may provide the individual with a powerful sword with which to confront troubling and potentially unreasonable data dissemination. Nevertheless, unless tempered in some way, these kind of peremptory rules risk destabilizing the nature and justification for a 'right to be forgotten' online which is fundamentally qualified rather than absolute in nature. These dilemmas have even been recognised within the EU, triggering, most notably, a preliminary reference that is currently before a Grand Chamber of the CJEU.[109]

7. Substantive Statutory Limitations related to Freedom of Expression

One important means of tempering these kind of inflexible rules is through recourse to explicit statutory provisions which limit the application of the default statutory framework on the grounds of freedom of expression. This freedom, in any case and as already emphasised, constitutes one of the primary counterweights to demands for a 'right to be forgotten' online. It is, therefore, vital to examine the presence of particular provisions within the G20 statutory data protection frameworks that establish specific limits applicable to this fundamental right. At the highest level of generality, these may be divided into those that limit the application of data protection generally and those which only restrict the circumstances in which data subjects can make use of certain *ex post* rights to limit or prohibit data processing. It is also important to consider both the precise scope of any freedom of expression activity that falls within these provisions and the depth of any limitation on data protection which they establish. The latter depends not only on the degree to which the provision enables an exemption from default data protection stipulations but also the substantive conditions that, in a number of cases, are attached to their use.

7.1 – Limitations related to the General Application of Substantive Data Protection

Aside from Indonesia and Mexico,[110] all of the G20 statutory data protection frameworks included provisions which explicitly limited the general application of data protection in the name of freedom of expression. However, aside from the singular case of Turkey,[111] these provisions were only made applicable to particular 'special' types of speech as opposed to freedom of expression in general.[112] Most restrictively, in three cases the limitations were restricted to journalism,

[108] Data Protection Regulation, section 9(1).

[109] C-136/17 *G.C. et. al. v Commission Nationale de l'Informatique et des Libertés* (CNIL). On 10 January 2019 Advocate General Szpunar handed down an Opinion in this case. See ECLI:EU:C:2019:14.

[110] Of course, even in Indonesia and Mexico, constitutional provisions do provide some safeguard to freedom of expression. However, even in the sensitive area of journalism, the data protection statute as written seems inconsistent with such protections since it makes no explicit attempt to accommodate itself to this right.

[111] The Turkish limitation applied not only to processing "for the purposes of art, history and literature or science" but also processing within the scope of freedom of expression". See Data Protection Law 2016, art. 28(1)(c).

[112] Article 85(1) of the EU GDPR did provide that "Member States shall be law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression". However,

sometimes defined through an institutional reference to the 'Press' or 'media' (Argentina,[113] Australia,[114] Korea[115]). At the national level, Germany similarly only mandated protection in relation journalistic purposes pursued by the institutional media.[116] However, a number of Länder extended their provisions to the pursuit by anyone of journalistic, literary and artistic expression.[117] This kind of wider specification of 'special' types of expression was the norm across most of the G20,[118] with six countries also extending this to cover certain types of scientific or academic speech (France,[119] Brazil,[120] Italy,[121] Japan,[122] Russia[123] and the UK[124]).

The substantive depth of these limitations was even more varied. In seven States the provisions set out were essentially absolute in their area of application (Argentina,[125] Australia,[126] Canada,[127] Japan,[128] Germany,[129] Korea[130] and (with the exception of academic expression) Brazil[131]). However, those benefiting from these provisions were still required to be publicly committed to a published privacy policy under Australian law,[132] to "strive to" take "necessary action to ensure the proper handling of personal information" under Japanese law[133] and (in the case of broadcasters and the online institutional media) to adhere to specified accuracy and access requirements under German law.[134] In three other States (South Africa,[135] Turkey[136] and the UK[137]), the provisions enabled all or almost all of the substantive data protection provisions to be dispensed with so long

aside from the special types of expression therein mentioned, this provision has yet to be implemented through specific provisions in any of the G20 EU countries.

[113] Personal Data Protection Act 2000, s. 1.

[114] Privacy Act, section 7(B)(4).

[115] Personal Information Protection Act 2011, art. 58(1)(4).

[116] Germany: Interstate Treaty on Broadcasting and Telemedia, ss. 9c and 57.

[117] See, for example, Brandenburg: Brandenburgishes Datenschutzgesetz (BbgDSG), s 29 and Mecklenburg-Vorpommern: Landesdatenshutzgesetz – DSG M-V, s 12.

[118] However, certain nuances remained in evidence. Thus, Japan did not expressly protect artistic activity whilst Brazil failed to include mention of literary expression. See Act on the Protection of Personal Information 2005, art. 76(1) (JAP) and General Data Protection Law, art. 4(II)(a) (BRA).

[119] Law no. 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties (as amended), art. 80.

[120] General Data Protection Law, art. 4(II)(b).

[121] Legislative Decree no. 196 of 30 June 2003 (as amended in 2018), art. 136.

[122] Act on the Protection of Personal Information 2005, art. 76(1)(iii).

[123] Data Protection Act 2006, art. 6(2)(6).

[124] Data Protection Act 2018, Schedule 2, Part V, s. 26(1).

[125] Personal Data Protection Act 2000, s. 1.

[126] Privacy Act, s. 7(B)(4).

[127] PIPEDA, s. 17(1).

[128] Act on the Protection of Personal Information 2005, art. 76(1)

[129] See Germany: Interstate Treaty on Broadcasting and Telemedia, ss. 9c and 57, Brandenburg: Brandenburgishes Datenshutzgesetz (BbgDSG), s 29 and Mecklenburg-Vorpommern: Landesdatenshutzgesetz – DSG M-V, s 12.

[130] Personal Information Protection Act 2011, art. 58(1)(4).

[131] General Data Protection Law, art. 4(II)(b).

[132] Privacy Act, s. 7(B)(4).

[133] Act on the Protection of Personal Information 2005, art. 76(1).

[134] See Germany: Interstate Treaty on Broadcasting and Telemedia, ss. 9c and 57

[135] Protection of Personal Information Act, No 4 of 2013, art. 7(1) and (3).

[136] Data Protection Law 2016, art. 28(1)(c).

[137] Data Protection Act 2018, schedule 2, Part V, para, 26(1).

as this was compatible with some kind of public interest test[138] and, in this regard, necessary for a balance to be achieved between competing rights. Lastly, provisions in the final group of three States (Russia,[139] France[140] and Italy[141]) established far-reaching public interest exemptions from rule-based restrictions such as those generally applicable to sensitive data but retained formal application of most of the core principles of data protection even within special areas of freedom of expression such as journalism.

7.2. Limitations relating only to *ex-post* Rights to Restrict or Prohibit Processing

Alongside the general clauses above, a number of G20 States also set out provisions restricting the ability of data subjects to use certain specified *ex post* injunctive rights to control processing (although not necessarily other remedies such as rights to compensation for damage caused by the ongoing illegal processing of data). In the EU G20 countries these limitations were explicitly justified on the basis of freedom of expression *simpliciter*, whilst a wider group of G20 States established limitations which implicitly protected a range of freedom of expression rights and interests. Turning first to the G20 EU countries (i.e. Germany, France, Italy and the UK), the GDPR itself establishes that the right to erasure/right to be forgotten (although not necessarily allied injunctive possibilities such as the right to object to processing[142]) did not apply to the extent that any such processing was necessary "for exercising the right to freedom of expression and information".[143] Interestingly, unlike the wider freedom of expression provisions in these States, this limitation was not restricted to special types of speech such as journalism. Turning to the wider group of countries, Mexico enabled such a claim to be refused where this was "necessary to carry out an action in the public interest",[144] whilst Argentina[145] and Korea[146] set out a similar limitation where the rights and legitimate interests of third parties would otherwise be harmed. Finally, the specific law adopted by Russia to enable an injunction on search engine indexing was triggered not by any illegal dissemination of personal data but only where the data was "unreliable" *("недостоверной")*, was "irrelevant" *("неактуальной")* or had "lost its value" ("утратившей значение") in light of either subsequent events or the applicant's subsequent actions.[147] The law also entirely excluded claims concerning information about unspent criminal convictions (including convictions which could never become spent).[148]

[138] Rather problematically, the Turkish law in this regard made reference to the need to ensure non-violation of "[the] privacy of personal life or personal rights" (concerns which are clearly at the heart of data protection) but also "national defence, national security, public safety, public order [and] economic safety" (Data Protection Law 2016, art. 28(1)(c)).
[139] Data Protection Act No. 152 FZ, art. 6(2)(6).
[140] Law no. 78-17 (as amended), art. 80.
[141] Legislative Decree no. 196 of 30 June 2003 (as amended in 2018), arts. 136-139 and Code of Conduct on the Processing of Personal Data in the Exercise of Journalistic Activities (as re-promulgated 2018).
[142] GDPR, arts. 18 and 21.
[143] Ibid, art. 17(3)(a).
[144] Federal Law on the Protection of Personal Data held by Private Parties, art. 26(V).
[145] Personal Data Protection Act 2000 25/326, s. 1.
[146] Personal Information Protection Act 2011, art. 37(2)(2).
[147] Federal Law of 13.07.2015 N 264-FZ, art. 10(3).
[148] Federal Law of 13.07.2015 N 264-FZ, art. 10(3).

8. Interplay with Statutory Liability Limitations for Online Platforms

Online platforms are generally not the original instigators of the publication of personal data. They are, however, not only implicated in the purely 'intermediary' storage and making available of content but also – and increasingly – in a whole range of "value-added operations"[149] including soliciting, organizing, combining, aligning and pushing content on to others. It is the pursuit of these further operations which can result in these platforms acquiring 'control' over this personal data and which, as section 3.2.2 above indicated, may well then mean that they fall within the scope of many G20 data protection laws. All these legal frameworks are predicated on the default assumption and expectation that the regulated entity will exercise full *ex ante* control over all processing of personal data within their systems. This constitutes a significant problem since expecting such comprehensive liability and responsibility for content will generally constitute a disproportionate interference with the activities of the online platforms and may even make their lawful operation all but impossible. Moreover, given that these actors are now so central to the dissemination of information online, this raises fundamental freedom of expression concerns which are separate and additional to the substantive issues discussed above. Therefore, notwithstanding that 'right to be forgotten' debate has generally sidestepped these issues by focusing only on question of *ex post* control, it is important to address this matter here.

Statutory 'intermediary' shields which potentially applied to a whole range of at least civil illegalities[150] were found in eleven out of fifteen G20 countries with established statutory data protection frameworks (namely, Brazil, France, Germany, Italy, Indonesia, Japan, Korea, South Africa, Turkey and the UK) (see Appendix Two for full details). The types of activities covered by these shields often remained either rather opaque or focused largely on passive or technical operations such as "relay[ing] others' communications with the use of specified telecommunications facilities"[151] or activity "consist[ing] of the storage of information provided by a recipient of the service".[152] As a result, the precise relationship between these shields and potential 'controller' duties under the parallel data protection framework was often unclear. This lack of clarity was explicitly highlighted in the scheme applicable to the four G20 countries within the EU. Thus, whereas on the one hand the e-Commerce Directive 2000/31/EC stated that it "shall not apply to (…)

[149] Van Hoboken, Joris, "The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember" (NYU, 2013) http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf

[150] Whilst no such legal provisions were found in the other five cases, statutory 'intermediary' shields in the area of intellectual property were located in Australia, Canada and Russia (see Appendix Two). Moreover, even in the other two cases (Argentina and Mexico) it was clear that courts have been seeking to establish certain 'intermediary' liability shields principles through case law. Whilst a detailed consideration of these developments go well beyond the scope of this article, excellent summaries are available within the Stanford Centre for Internet and Society's World Intermediary Liability Map, https://wilmap.law.stanford.edu/ .

[151] Japan: Act on the Protection of Personal Information 2005, art. 2(iii).

[152] European Union Directive 2000/31/EC, art. 14(1). See Appendix Two for details of laws implementing this Directive in France, Germany, Italy and the UK. Similar wording was also found in South Africa, although the law here did also shield "information location tools, including a directory, index, reference, pointer or hyperlink" (Electronic Communications and Transactions Act 2002, art. 76).

questions relating to information society services covered by [data protection legislation]",[153] the General Data Protection Regulation 2016/679 provided that it "shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive".[154]

Even once engaged, the strength of these provisions also exhibited some divergence. In eight out of ten cases the shields appeared to provide for some kind of 'notice and takedown' regime whereby the provider would be shielded from most forms of liability so long as it could be notified about illegalities within its service and took action to remove or disable access to information once it acquired knowledge of a legal problem. However, variations remained apparent even within this group including, for example, whether actual or merely constructive knowledge of a problem would lead to liability, what form any notification should take and whether information about claims should be passed on to any original publisher. For example, in Korea, a pure 'notice and takedown' procedure sat in an unclear relationship with a requirement for service providers as a "temporary measure" to block access to information whenever it was "difficult to judge whether information violates any right" or "it is anticipated that there will probably be a dispute between interested parties".[155] Meanwhile, in Turkey the 'notice and takedown' procedure similarly sat alongside the right (after one week of inaction) to obtain a binding removal order from a magistrate within three days. Failure by the person in charge of the service to comply with such an order (within two days) was made an imprisonable criminal offence.[156] Provisions in two final cases of Brazil and Indonesia generally established immunity even after 'notice' so long as a court order had not been obtained which specifically ordered action. Thus, aside from the non-consensual disclosure of "materials containing nudity or acts [of a] sexual private character" (where a 'notice and takedown' procedure was provided),[157] the Brazilian law established that "the provider of Internet applications can only be liable for civil damages arising out of content generated by third parties if it does not act, after specific court order, within the framework and technical limits of its services and timely mentioned, to make the content identified as infringing unavailable, except for contrary established statutory provisions".[158] Rather similarly, the law in Indonesia established that an Electronic System Operator would have to remove information disseminated on its services after a "court determination" ("*penetapan pengadilan*").[159] Interestingly, and mirroring the precise concerns of the *Google Spain* litigation, this provision did also establish that such a determination could provide for the removal of information which was found to be "irrelevant" ("*yang tidak relevan*"),[160] presumably notwithstanding that its initial dissemination or publication in another context might remain entirely legal.

[153] European Union Directive 2000/31/EC, art. 1(5)(b).
[154] European Union General Data Protection Regulation 2016/679, art. 2(4).
[155] Act on Promotion of Information and Communications Network Utilization and Information Protection, arts. 44-2. In addition, the law appeared to envisage an even more proactive approach being taken to certain categories of personal information "such as resident registration numbers, account numbers and credit card information" (Ibid, art. 32-3).
[156] Law no. 5651 (Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications), art. 9(2) and (4).
[157] Brazil, Marco Civil da Internet, art. 21.
[158] Ibid, art. 20.
[159] Law of the Republic of Indonesia No. 11 of 2008 Concerning Electronic Information and Transactions, art. 26(3) (as amended in 2016).
[160] Law of the Republic of Indonesia No. 11 of 2008 Concerning Electronic Information and Transactions, art. 26(3) (as amended in 2016).

9. Summary and Discussion of Findings

A need for an online 'right to be forgotten' has clearly been championed by the EU data protection regime, both through judicial decisions such as *Google Spain* and through the explicit reference to this phraseology within the new General Data Protection Regulation 2016/679. However, our analysis demonstrates that the basic statutory underpinnings of this concept are present in the great majority G20 countries. Although the powerhouses of China, India and the United States still constitute important exceptions in this regard, fifteen out of the nineteen G20 States (almost 80%) have now adopted data protection laws which establish a general framework for most forms of personal data processing. Moreover, all of these laws include rectification rights enabling individuals to require action in relation to 'inaccuracy' and all bar one explicitly empower individuals to raise broader challenges as regards the legitimacy of an ongoing dissemination of personal data. Moreover, eleven of these States have enacted broad statutory 'intermediary' liability shields which could help justify why certain actors such as online platforms and search engines may be largely exempted from *ex ante* duties here but nevertheless may still be required to respond to *ex post* injunctive requests.

Despite this, the challenges in this area should not be underestimated. Firstly, the exact scope of many G20 data protection frameworks remains rather opaque especially in an online context. In particular, almost all these laws exempt certain kinds of processing carried out by amateur individuals in the context of their private life. This is eminently understandable given both the limited "expertise and resources" such individuals typically possess and the fact that, historically, data protection laws were largely crafted to respond to "risks resulting from the processing of personal data by governmental and commercial institutions".[161] However, it must be recognised that amateur individuals are "in many cases the primary perpetrators of privacy infringements" online at least within "social networking sites" and similar environments.[162] It, therefore, seems unlikely that these exemptions should shield such individuals from being held directly accountable whatever the circumstances. Indeed, well outside of the EU-context, many of these laws explicitly state that the exemption is conditional on the rights of others not being (unduly) infringed or, even more restrictively, categorically exclude its application where personal data is subject to a disclosure to third parties. Of even more practical importance, the increasingly active role of online platforms in both shaping and spreading such disclosures may well render these actors 'controllers' of at least some of the resultant processing. Indeed, as regards internet search engines specifically, this was the central and seminal holding of the Court of Justice of the EU in *Google Spain*. Secondly, an axiomatic aspect of our understanding is that the 'right to be forgotten' is a qualified claim which should be defeated when continued processing is justified by compelling reasons related, most especially, to freedom of expression. However, at least in relation to so-called 'sensitive' data, the great majority of G20 data protection laws set out default rules which, on their face, appear unsuited to the necessary flexible interpretative approach. On the other hand, thirteen out of fifteen these laws did set out some kind of discrete freedom of expression limitation. However, the vast majority of these only shielded 'special' types of speech such as journalism, thereby potentially

[161] Van Alsenoy, Brendan, "I tweet therefore I am … subject to data protection law?"(2016), https://www.law.kuleuven.be/citip/blog/i-tweet-therefore-i-am-subject-to-data-protection-law/.

[162] Helberger, Natali and Joris van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers' Computer Law Information (2010), pp. 101-9, 103.

excluding large swathes of expressive activity on social media and through technical tools such as search engines. Moreover, within their area of application, approximately half of these provisions are essentially absolute in nature, thereby raising the prospect of another type of 'unbalanced' outcome. Finally, even in the G20 countries with wide-ranging statutory 'intermediary' shields, their precise relationship with potential 'controller' responsibilities under data protection generally remained deeply opaque. Furthermore, these shields were found to be entirely lacking in four out of the fifteen (c. 25%) G20 countries that had enacted statutory data protection law.

However, whilst undoubtedly formidable, these challenges are far from necessarily fatal to the development a 'right to be forgotten' online through data protection. To the contrary, they are all being confronted within the EU data protection regime which post-*Google Spain* has indubitably embarked down such a path. Thus, the new General Data Protection Regulation 2016/679 not only continues with an exemption for processing "by a natural person in the course of a purely personal or household activity"[163] but includes a new recital which states both that this "could include … social networking activity undertaken within the context of such activities" and that the Regulation will continue to apply to "controllers and processors which provide the means for processing personal data for such personal or household activities".[164] It will be up to the Court of Justice of the EU to interpret this exemption in light not only of this new recital but also the wider aims of European data protection.[165] Secondly, a Grand Chamber of the Court of Justice is currently considering how in the context of search engine indexing the apparently peremptory rules applicable to 'sensitive' (and to a lesser extent inaccurate) data should be construed given the general understanding that the 'right to be forgotten' should be qualified.[166] Meanwhile, reflecting the need for a balanced approach, the Court has recently cast doubt[167] on the legitimacy of absolute or near-absolute exemptions for journalism and cognate 'special' forms of expression (concepts which it, in any case, has already found are not broad enough to directly include activities such as search engine indexing).[168] In the future, the Court will also undoubtedly have to construe the (as yet largely unimplemented) instruction that EU States to "by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information"[169] even outside of 'special' form of expression, as well as bar on the use of the right to erasure when processing is necessary "for exercising the right of freedom of expression".[170] Both of these represent innovations within the new GDPR instrument. Finally, whilst the Google Spain judgment did not directly invoke the e-Commerce Directive 2000/31 'intermediary' shields, it nevertheless held (apparently on the wider grounds of avoiding a disproportionate result) that search engines would only acquire data protection responsibilities insofar as they were "liable to affect significantly, and additionally compared with that of the [original] publishers… the fundamental rights to privacy and to the protection of personal data" and, even then, would only be

[163] Regulation 2016/679, art. 2(2)(a).
[164] Ibid, recital 18.
[165] For one approach to construing the personal exemption here see David Erdos, 'Beyond "having a domestic"? Regulatory interpretation of European Data Protection Law and individual publication' 33 (2019) Computer Law and Security Review 275 at pp. 290-292.
[166] C-136/17 *G.C. et. al*.
[167] In sum, in C-345/17 *Buivids* it held that even within this area it must be examined whether any derogations are "necessary in order to reconcile the right to privacy with the rules governing freedom of expression, and whether those exemptions and derogations are applied only in so far as is strictly necessary" (at [68]).
[168] C-131/12 *Google Spain* at [85].
[169] Regulation 2016/679, art. 85(1).
[170] Ibid, art. 17(3)(a).

required to act "within the framework of its responsibilities, powers and capabilities".[171] Potentially, somewhat similar 'intermediary' limitations may be applied to other online platforms such as social networking sites.[172] In the future, the Court will need to construe the new provision in the GDPR which (albeit in a rather opaque manner) seeks to establish a relationship between data protection and the statutory 'intermediary' shields set out within e-Commerce law.

The fact that at least the EU is, and will continue to, grapple with these difficulties does not mean that the legal results will necessarily be ideal. To the contrary, given a profoundly challenging socio-technological and an imperfect legal environment, these results are almost certain to remain decidedly second best. Nevertheless, it is now clear that the essential nature of the EU's data protection framework does mandate such an attempt. According to the analysis presented in this paper, much the same is true in the great majority of other countries within the G20 with statutory data protection frameworks. In that context, it should also be reiterated that at a practical level "[d]ata protection and related researchers have long noted the increase in threats and content issues for individuals in the online environment"[173] and found that "these issues are causing problems for children, teenagers and adults worldwide, not merely those in the EU".[174]

Seen from the two vantage points above, it should be clear why the manifest tension between freedom of expression and data protection online should not lead to the former trumping the latter in most or all cases, simply as a result of the latter being largely ignored in reality. Instead, there is a strong case for attempting to craft proportionate and effective outcomes here, initially through the interpretation and application of existing law and ultimately through new legislative initiatives. In light of the worldwide nature of information flows especially online, such an initiative must be transnational. Moreover, given their current dominance within the global economy and society, the countries within the G20 could potentially play a key role to play here. It would, therefore, be valuable if issues connected to the 'right to be forgotten' online were integrated in to the G20's existing programme on the Digital Economy. G20 Data Protection Authorities (DPAs) should also consider meeting on the fringes of relevant G20 events in order to share good practice within these and related areas. In any case, these regulators should commit to seeking an active and balanced application of their laws to the various online data protection concerns which are epitomised in the evolving concept of the 'right to be forgotten' online.

[171] C-131/12 *Google Spain* at [38].
[172] For a general discussion see David Erdos, 'Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU *acquis*', *International Journal of Law and Information Technology* (Vol. 26(3), pp. 189-225) (2018).
[173] Lambert, Paul, *The Right to be Forgotten* (Bloomsbury, 2019), 15.
[174] Ibid, 16.

Appendix 1: Statutory Data Protection Law within the G20

State	Law	Location
Africa		
South Africa	Protection of Personal Information Act, No 4 of 2013 (PPIA)	https://www.saica.co.za/Portals/0/Technical/LegalAndGovernance/37067_26_11_Act4of2013ProtectionOfPersonalInfor_correct.pdf (English)
Asia-Pacific		
Australia	Privacy Act 1988	https://www.legislation.gov.au/Details/C2018C00034 (English)
China	The Decision of the Standing Committee of the National People's Congress on Strengthening Internet Information Protection' (SC-NPC Decision 2012)	http://www.law.hku.hk/cprivacy/archives/189 (English)
	Information Security Technology - Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems (MIIT Guidelines 2013)	https://chinacopyrightandmedia.wordpress.com/2013/01/21/information-security-technology-guidelines-for-personal-information-protection-on-public-and-commercial-service-information-systems/ (English)
	Cybersecurity Law of the People's Republic of China (2016)	https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (English)
	China's Personal Information Security Specification (2018)	https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/ (English)
India	Information Technology Act 2000 (IT Act 2000)	https://meity.gov.in/content/information-technology-act-2000-0 (English)
	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules 2011)	http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf (English)
Indonesia	*Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (Data Protection Regulation)*	https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016 (Original Language)
Japan	Act on the Protection of Personal Information 2005 (APPI)	https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf (English)
Korea	Personal Information Protection Act 2011 (PIPA)	http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf (English)
Saudi Arabia	N/A	N/A
Europe		
EU	General Data Protection Regulation 2016/679	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG (English)
France	*Law n° 78-17 of 6 January 1978 on information technology, data files and individual liberties (amended as of 30 August* 2019)	https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 (Original Language)
Germany	Federal Data Protection Act	https://www.gesetze-im-internet.de/englisch_bdsg/ (English)

	Interstate Treaty on Broadcasting and Telemedia (only ss. 9 and 57 relevant)	https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Rundfunkstaatsvertrag_RStV.pdf (Original Language)
Italy	*Legislative Decree no. 196 of 30 June 2003 (as amended by Legislative Decree 10 August 2018, n 101)*	https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.6 (Original Language)
	Code of Conduct on the Processing of Personal Data in the Exercise of Journalistic Activities (as re-promulgated 29 November 2018)	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9067692
Russia	Federal Personal Data Law No. 152 FZ (as amended by Federal Law of 25.11.2009)	https://iapp.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf (English)
	Federal Law of 13.07.2015 N 264-FZ "On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection'"	http://www.consultant.ru/document/cons_doc_LAW_182637/ (Original Language)
Turkey	Data Protection Law 2016 (DPL)	https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/ (English)
UK	Data Protection Act 2018	http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (English)
North America		
United States	US Civil Code	https://uscode.house.gov/ (English)
Canada	Personal Information Protection and Electronic Documents Act	http://laws-lois.justice.gc.ca/eng/acts/P-8.6/ (English)
South America		
Argentina	Personal Data Protection Act 2000 25/326	http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf (English)
Brazil	General Data Protection Law 2018	https://iapp.org/resources/article/brazils-general-data-protection-law-english-translation/ (English)
Mexico	Federal Law on the Protection of Personal Data held by Private Parties (2010)	https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf (English)
	Amended Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (2017)	*http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf (Original)*

Appendix 2: Statutory Intermediary Shields within the G20 (including specific to copyright)

State	Law	Location
Africa		
South Africa	Electronic Communications and Transactions Act, 2002	http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/South%20Africa/ElecComm.PDF (English)
Asia-Pacific		
Australia	Trade Agreement Implementation Act 2004 (Cth) Sch 9	https://www.legislation.gov.au/Details/C2004A01355/ (English)
	Copyright Legislation Amendment Act 2004 (Cth) Sch 1	https://www.legislation.gov.au/Details/C2004A01389 (English)
China	Interpretation No. 20 [2012] of the Supreme People's Court	http://en.pkulaw.cn/display.aspx?cgid=191740&lib=law (English)
India	Information Technology Act 2000, s. 79	https://meity.gov.in/content/information-technology-act-2000 (English)
Indonesia	Law of the Republic of Indonesia No. 11 of 2008 Concerning Electronic Information and Transactions	http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e.html (English)
	Law of the Republic of Indonesia No. 19 of 2016 Concerning Amendment to Law of the Republic of Indonesia No. 11 of 2008 Concerning Electronic Information and Transactions	https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf (Original Language)
	Ministerial Circular Letter Number 5 of 2017 ("SE 5/2017")	https://jdih.kominfo.go.id/produk_hukum/view/id/558/t/surat+edaran+menteri++komunikasi+dan+informatika+nomor+5+tahun+2016+tanggal+30+desember+2016 (Original Language)
Japan	Act No. 137 of 2001 on the Limitation of Liability for Damages of Specified Telecommunications Service Providers	http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=02&re=01 (English)
Republic of Korea	Act on Promotion of Information and Communication Network Utilization and Information Protection	http://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG (English)
	Copyright Law, art. 102	https://www.wipo.int/edocs/lexdocs/laws/en/kr/kr058en.pdf (English)
Saudi Arabia	N/A	N/A
Europe		
EU	E-Commerce Directive 2000/31 (see below for implementation in France, Germany, Italy and the UK)	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031 (English)

France	*LCEN 2004-575*	http://www.wipo.int/wipolex/en/details.jsp?id=12761 (Original Language)
Germany	Telemedia *Act 2007*	http://www.wipo.int/wipolex/en/text.jsp?file_id=462253 (Original Language)
Italy	*Legislative Decree N. 70, April 9, 2003*	http://www.parlamento.it/parlam/leggi/deleghe/03070dl.htm (Original Language)
Russia	Federal Law No. 187-FZ	https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru099en.pdf (English)
Turkey	Law no. 5651 (Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications)	http://www.wipo.int/edocs/lexdocs/laws/tr/tr/tr101tr.pdf (English)
UK	The Electronic Commerce (EC Directive) Regulations 2002	http://www.legislation.gov.uk/uksi/2002/2013/contents/made (English)
North America		
United States	Communications Decency Act 1996	https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapII-partI-sec230.htm (English)
Canada	Copyright Modernization Act, SC 2012, c 20	http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/page-2.html#docCont (English)
South America		
Argentina	N/A	N/A
Brazil	Marco Civil Da Internet, Federal Law no. 12.965, April 23, 2014	https://docs.google.com/document/d/1kJYQx-l_BVa9-3FZX23Vk9IfibH9x6E9uQfFT4e4V9I/pub (English)
Mexico	N/A	N/A