NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 22, ISSUE 4: MAY 2021

GOOGLE LLC V. CNIL: THE LOCATION-BASED LIMITS OF THE EU RIGHT TO ERASURE AND LESSONS FOR U.S. PRIVACY LAW

***Sam Wrigley**[*] **& Anne Klinefelter**[**]*

As the United States considers preemptive federal privacy law, the discussion can be enriched by a reassessment of the EU example as illustrated in a 2019 decision at the European Court of Justice. The General Data Protection Regulation that took effect in 2018 is often described as an important model for unifying and centralizing data protection law in order to provide consistent protections of rights. But the Google LLC v. CNIL *decision highlights that the EU law did not in fact create a monolithic system without room for Member State variation.*

This Article takes a close look at the way that the erasure right is articulated in the GDPR, examining how competing rights are balanced, how Member States' different approaches to balancing rights are accommodated, and how related provisions in the law inform an understanding of the erasure provision in Article 17. This Article also examines the 2019 Google LLC v. CNIL *decision, exploring the Court's reasoning and the impact of the case on EU erasure rights and beyond.*

This Article draws on these examinations of the erasure-related provisions of the GDPR and of the Google LLC v. CNIL *decision to advance a better understanding of how the influential EU*

[*] Doctoral Candidate at the University of Helsinki, Finland. Many thanks to those who helped to improve this Article, including (but not limited to) co-author, Anne Klinefelter, those at NC JOLT and the people at the University of Helsinki. Any errors contained remain the fault of the authors.

[**] Henry P. Brandis Distinguished Professor of Law and Director of the Law Library, University of North Carolina. Thanks to my research assistant Shannon Coy, my co-author Sam Wrigley, and Professor Päivi Korpisaari for inspiration for this Article. Thanks as well to the Fulbright Finland Foundation, the Faculty of Law at the University of Helsinki, and the UNC School of Law and Kathrine R. Everett Law Library for generous support for my visit to Finland that led to this article. Thanks to Christine Xiao and Lily Faulconer for helpful editing and for an engaging symposium.

Regulation embraces the possibility of significant Member State variation and ongoing balancing of data protection with expression and information rights. Guiding principles of subsidiarity and proportionality that are foundational to the European Union, incorporated into the GDPR, and evident in the Google LLC v. CNIL *decision provide the basis for this national deference and deferred balancing. Together, subsidiarity and proportionality principles caution against extensive consolidation of privacy law into a one-size-fits-all solution. The United States can learn from the European Union that a monolithic and inflexible federal law may not only be difficult to enact but also undesirable.*

TABLE OF CONTENTS

I. INTRODUCTION

The Internet presents challenges for the territoriality of law. Within EU data protection law, the right to erasure, also known as the right to be forgotten, is challenged by borderless aspects of the Internet. This right has developed in the context of internet search engines, and the fact that personal name searches increase the exposure of information protected by EU data protection law. The EU erasure right can require that search engines de-index protected personal information, but implementation can be seen as pitting effectiveness of the remedy against jurisdictional authority given the accessibility of different versions of search engines across legal boundaries.[1] Imagine that a French citizen without any aspirations of fame or public office discovered that a Google search for their name surfaced, for example, a long-ago arrest for charges later dropped or a statement which the person made as a child. The citizen, aware that EU law provides strong protections for limiting the processing or control of personal information, may wish this information to be removed from search results and so attempt to exercise their right to erasure under the General Data Protection Regulation ("GDPR"), Article 17.[2]

Assuming that the citizen can successfully show one of the grounds for erasure, Google (if it wished to try to do so) would then have to assert that its processing was nonetheless justified under one of the permitted GDPR grounds, e.g., by showing a countervailing right of expression or of access to information. Absent a successful assertion, any continued processing of that data by Google would be in violation of the French citizen's right to erasure. The French citizen, however, may wish to go further than simply having the information removed from the version of Google which targets France and may want to have these search results banished from all

[1] For a classic piece on the difficulties of law and the global internet, see Peter Swire, *Of Elephants, Mice, and Privacy: International Choice and Law and the Internet*, 32 INT'L. L. 991 (1998).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter the GDPR].

versions of Google Search; they might not, for example, want this information displayed to persons using the German or U.S. versions of Google, nor to French persons who might stray from the French version of Google Search to use another national version.

This question of territoriality, and the inherent questions of how to provide effective data protection, were ones the French data protection authority, *la Commission Nationale de l'Informatique et des Libertés* ("CNIL"), faced, and its response was to assert that de-indexing should happen in all versions of Google search engines.[3] One can imagine that some multi-national actors might have acquiesced, if only to simplify compliance with a consistent implementation in all services. But Google instead pushed back on global implementation of erasure rights for search engines.[4] Faced with a question of how to interpret EU law, France referred the point of territoriality of the erasure right under the GDPR to the European Court of Justice ("ECJ").[5]

In the fall of 2019, in *Google LLC v. CNIL*,[6] the ECJ delivered a judgment finding significant location-based limits to the EU right to erasure.[7] The Court not only rejected the French authority's assertion that French citizens could automatically assert the right worldwide, but also denied automatic pan-EU implementation of these types of erasure claims.[8] The judgment of the Court does not provide perfect clarity on all the territoriality issues for erasure, but it does offer important guidance for U.S. multinational actors and several lessons for the United States as the need for broad preemptive national privacy legislation is debated. To reach its decision, the EU Court addressed one of the core complications of privacy and data protection law—the tension between those rights and the freedoms of expression and access to information.[9] While

---

[3] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶ 30 (Sept. 24, 2019) (judgment).

[4] *Id.* ¶¶ 31, 38.

[5] *Id*. ¶ 39.

[6] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019) (judgment).

[7] *Id*.

[8] *Id*. ¶¶ 40–73.

[9] *See, e.g.*, *id*. ¶ 60.

some of the GDPR represents conclusions about how to balance these rights and freedoms, some of that hard work was explicitly left for Member States to address through potentially varying national laws and through procedures for harmonization that rely on consultation among Member States' designated data regulators. These dual sets of balancing acts, for competing rights and competing legal authorities, can be instructive to the United States which struggles with the same tensions.

Scholars have already developed a body of work analyzing and comparing forms of federalism in the European Union and in the United States and comparing federal systems of privacy or data protection law specifically.[10] This Article advances that conversation regarding how to balance freedoms and how to balance national and state law using the example of search engine erasure location-based limits recognized by the ECJ in the *Google LLC v. CNIL* decision. This analysis is particularly salient given ongoing discussions about the desirability of new omnibus-style federal privacy or data protection law in the United States.[11]

This Article brings together an author from the United States and an author from the European Union to analyze the 2019 ECJ decision about the territoriality of the right to erasure and to consider some lessons for the U.S. debate about potential omnibus federal privacy legislation that would preempt an expanding set of state

[10] *See, e.g.*, THE FEDERAL VISION: LEGITIMACY AND LEVELS OF GOVERNANCE IN THE UNITED STATES AND THE EUROPEAN UNION (Kalypso Nicolaidis and Robert Howse eds., 2003) (ebook) (examining and comparing federalism principles and systems in the United States and in the European Union); FEDERALISM AND SUBSIDIARITY: NOMOS LV (James E. Fleming and Jacob T. Levy eds., 2016) (ebook) (addressing U.S. federalism in law and government with comparative analysis of European models); Paul Schwartz, *Preemption and Privacy*, 111 YALE L. J. 902 (2009) (advising against broad preemptive federal privacy law); Bilyana Petkova, *The Safeguards of Privacy Federalism,* 20 LEWIS & CLARK L. REV. 595 (2016) (noting benefits of state privacy law innovations).

[11] *See* Omer Tene, *GDPR's Second Anniversary: Cause for Celebration and Concern,* INT'L ASSOC. OF PRIVACY PROS. PRIV. PERSPECTIVES BLOG (May 26, 2020), https://iapp.org/news/a/gdprs-second-anniversary-a-cause-for-celebration-and-concern/ [https://perma.cc/FU32-N8SN] (discussing the impact of the GDPR including on U.S. law and observing "[o]ne of the thorniest policy issues impeding the progress of U.S. privacy legislation is the scope and degree of preemption of state privacy laws.").

laws.[12] Section II of this Article explores the *Google LLC v. CNIL* judgment and its grounding in both EU data protection law and EU law more generally as articulated by the ECJ consensus judgment. Section III considers lessons for the United States regarding the principles of subsidiarity and proportionality that shape the backdrop for this erasure decision. The Article concludes with the recommendation that the United States incorporate similar moderating concepts as pre-emptive national legislation for privacy or data protection is considered.

II. *GOOGLE LLC V. CNIL*: LOOKING TO CASE AND CONTEXT

A. Statute

The starting point for the right to erasure is set out by the GDPR, Article 17(1), which states where one of the (closed list of) statutory grounds applies, data subjects "shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay."[13] This right is positioned as part of the EU's protection of both privacy and data protection as

[12] The conflation of privacy law with data protection law elides important distinctions between the purpose, scope, and remedies for these interests. *See* Dan Solove, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477, 486 (stating that privacy is "an umbrella term" and mapping problematic activities that include information collection, processing, and dissemination as well as intrusions and decisional interferences); BART VAN DER SLOOT, THE GENERAL DATA PROTECTION REGULATION IN PLAIN LANGUAGE 40 (2020) ("Although the right to data protection was initially still closely connected to the right to privacy, it has gradually become an increasingly independent doctrine, especially in the European Union."); Sam Wrigley, *The Mysterious Nature of Data Protection as a Qualified Right: A Problem of Scope and Purpose?* In *Oikeuksia, Vapauksia ja Rajoituksia: Viestintäoikeuden vuosikirja 2019*, HELSINGIN YLIOPISTO, OIKEUSTIETEELLINEN TIEDEKUNTA 127, 127–58 (Päivi Korpisaari ed., 2020). This article does not attempt to resolve this definitional problem. Because the related interests are generally referred to as "privacy" interests in the United States, this article uses this term for U.S. law. Although the ECJ Court refers to both privacy and data protection rights at various points in the *Google LLC v. CNIL* decision, this article uses the term "data protection" to ground its analysis in the EU data protection law that is interpreted in this case.

[13] The GDPR, *supra* note 2, at art. 17(1).

fundamental rights, as protected by the Charter of Fundamental Rights of the European Union ("Charter").[14] However, neither these fundamental rights nor the right to erasure exist in isolation. In particular, the European Union also provides a Charter right protecting the freedom of expression and information.[15] Given the obvious potential for conflict between these rights, it is unsurprising that the GDPR, Article 17(3), which sets out the exceptions to the right to erasure, contains an explicit exemption for processing activities that are necessary to exercise one's freedom of expression and information under sub-paragraph (a).[16]

At first glance, the exception in Article 17(3)(a) is quite wide; the statute states that the right to erasure "shall not apply to the extent that processing is necessary for exercising the right of freedom of expression and information."[17] However, Article 17(3)(a), by itself, is an incomplete picture for two reasons. First, as will be discussed below, the EU's obligation towards the balancing of these competing rights does not begin with the application of legislation; it must also be considered during the actual drafting of EU law. It is therefore necessary to examine Article 17(1), which sets down the conditions under which the right to erasure can be imposed, in order to gain a fuller picture. Secondly, merely because Article 17(3)(a) has the potential to suspend the application of Article 17(1), this will not always be the case. It is therefore necessary to examine how the two provisions actually interact.

It is also important to note that the GDPR contains a specific provision which imposes a duty on Member States to "reconcile" data protection with the freedom of expression and information under Article 85.[18] Because the obligation is on a Member State level, the GDPR accepts that certain questions of freedom of expression and information may vary from one country to another. The exact way in which different Member States have implemented

---

[14] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1 [hereinafter The Charter]. Respect for private and family life, and the protection of personal data are enshrined as separate rights under Arts. 7 and 8, respectively.

[15] The Charter, *supra* note 14, at art. 11.

[16] The GDPR, *supra* note 2, at art. 17(3)(a).

[17] *Id.* at art. 17(3)(a).

[18] *Id.* at art. 85.

this provision will not be explored in this Article, but the mere existence of this provision will be helpful to remember, as it makes clear that the balancing of the right to erasure with the freedoms of expression and information may play out differently, depending on the specific countries involved.

1. Laying Down the Law

Under its legislative procedure,[19] the European Union is required to consider the impact of any proposed law on fundamental rights,

[19] The European Union's legislative procedure is primarily governed by the Consolidated Version of the Treaty on the Functioning of the European Union art. 15, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter TFEU], Part Six Institutional and Financial Provisions, Chapter 2 Legal acts of the Union, adoption procedures and other provisions. Under art. 289, the ordinary legislative procedure requires that, *inter alia*, regulations are proposed by the European Commission and then adopted by the European Council and the European Parliament. To help reach this agreement, the ordinary legislative procedure includes a conciliation phase under art. 294(10)–(12) and the various European Institutions will also have informal "trilogue" meetings. For more, see EUROPEAN PARLIAMENT, A GUIDE TO HOW THE EUROPEAN PARLIAMENT CO-LEGISLATES UNDER THE ORDINARY LEGISLATIVE PROCEDURE (2014). It is also worth noting that the European Ombudsman held a strategic inquiry on the transparency of the trilogue procedure and found that there were a number of shortcomings, including a lack of publication of documents. EUROPEAN OMBUDSMAN, DECISION OF THE EUROPEAN OMBUDSMAN SETTING OUT PROPOSALS FOLLOWING HER STRATEGIC INQUIRY OI/8/2015/JAS CONCERNING THE TRANSPARENCY OF TRILOGUES *passim* (2016). While some attempts have been made to improve access to these documents (*see*, *e.g.*, T-540/15 *De Capitani v European Parliament*, ECLI:EU:T:2018:167), there is still a long way to go (*see*, *e.g.*, Gijs Jan Brandsma, *Transparency of EU Informal Trilogues Through Public Feedback in the European Parliament: Promise Unfulfilled*, 26 J. OF EUR. PUB. POL'Y 1464 (2018) (scrutinizing the level of public accountability in the EU legislative process and finding it fails to meet requirements which undermines the legitimacy of the process)). Fortunately, as the GDPR was a very high-profile piece of legislation, many documents from the legislative process are available, but the amount of available information is far from complete. *See, e.g.*, *2012/0011(COD): Personal Data Protection: Processing and Free Movement of data (General Data Protection Regulation)*, EUR. PARLIAMENT LEGIS. OBSERVATORY, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011 [https://perma.cc/5JNH-4J44] (COD) (last visited May 11, 2020) (containing a document gateway for the GDPR).

including those as expressed in the Charter.[20] If doing so reveals that the law in question may restrict a Charter right or freedom, that law may only be passed if it complies with the requirements in the Charter, Article 52, which states that "any limitation" on such rights and freedoms must "respect the essence of those rights and freedoms," be "subject to the principle of proportionality," be "necessary," and "genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[21]

As can be seen from a GDPR trialogue document,[22] Article 17 was subject to significant variation and debate during the EU legislative procedure.[23] While much of the content of the discussion is not available, it is known that, *inter alia*, the consequences for the freedom of expression was a live issue during the debate in the Council stage of the legislative process.[24] During that stage, the

[20] Under the Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter TEU], art. 6, the Charter has the "same legal value" as the EU Treaties. The practical consequence of this is that the European Union cannot pass any legislation which violates the Charter and therefore any such legislation is outside of the European Union's competences and so invalid. *See also* the Charter, *supra* note 14 at art. 51 (requiring EU Institutions to have "respect the rights, observe the principles and promote the application [of Charter rights] thereof in accordance with their respective powers."

[21] The Charter, *supra* note 14, at art. 52.

[22] Regulation (EU) No XXX/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), trialogue 4-Column Table (2016), https://www.europarl.europa.eu/committees/en/data-protection/product-details/20120514CDT45071 [https://perma.cc/ULV6-2KGU].

[23] *Id*.

[24] As noted *supra* note 8, the EU legislative procedure suffers somewhat from a lack of transparency. In particular, there is no consistent release of legislative debates throughout EU Institutions; while the European Parliament releases reports of its debates in *European Parliamentary Debates*, the Commission and the Council do not do so. That is not to say that there are no resources available; the Council does live-stream its debates and publish minutes and agendas, and both Institutions publish summary documents and reports (e.g., the Council's Common Positions or Statements of the Council's Reasons, and the

Council noted that, in relation to Article 17(1)(a), the Commission had "emphasised that its proposal was in no way meant to be a limitation of the freedom of expression."[25] It is therefore reasonable to assume that, at least to some extent, the EU legislative bodies have attempted to fulfill their task of balancing the right of data protection against the freedom of expression and information while drafting Article 17(1), even before reaching the exception contained in Article 17(3)(a).

If, for the sake of argument, it is accepted that the European Union has properly performed this balancing test, then it can also be assumed that, at least in theory, Article 17(1) has already been balanced such that it will not permit erasure where that would leave the freedom of expression and information inevitably and unjustifiably restricted.[26] What, then, is the role for Article 17(3)(a), and why is this secondary balancing act required? In order to analyze the provision fully, it is first necessary to consider the scope of Article 17(1). This paragraph states that a data subject shall only have the right to obtain erasure if one of the following grounds exist:

> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
> (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
> (d) the personal data have been unlawfully processed;

Commission's Communication documents). However, the level of detail in and utility of these sources can vary dramatically.

[25] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), revised and consolidated draft, Interinstitutional File: 2012/0011 (COD), 15395/14 (2014), 102 *et seq*.

[26] If this were found not to be the case and the provision were found to contravene the Charter's balancing requirements then it could simply be challenged and found invalid under the TFEU, arts. 263 and 264.

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).[27]

This new, statutory implementation bears some welcome differences from the right to erasure as formulated by the ECJ in *Google Spain*,[28] which was based on the now-repealed Data Protection Directive ("DPD").[29] The case, now being somewhat infamous, may need little introduction, but it is valuable to make some notes before continuing. In particular, the Court in *Google Spain* did not claim to invent the concept of erasure; rather, the right in that specific case was treated as being the logical consequence of two provisions in the DPD, being Article 12 (titled the "Right of access") and Article 14 (titled "The data subject's right to object").[30] In particular, Article 12(b) gave data subjects the ability to demand "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive."[31] In the specific facts of the case, the relevant personal data was being processed under the grounds of legitimate interest and, under Article 14(a), data subjects also had the right to "object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[32] In the ECJ's judgment, once such an objection had been appropriately made, the data could no longer be lawfully processed, and Article 12(b) must therefore allow appropriate erasure of the data.[33]

On one level, this judgment should not be considered particularly controversial; the law explicitly said that data subjects

---

[27] The GDPR, *supra* note 2, at art. 17(1).

[28] Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos (AEPD) (C-131/12 *Google Spain SL*), ECLI:EU:C:2014:317 (May 13, 2014).

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 31 [hereinafter the DPD].

[30] C-131/12 *Google Spain SL*, ¶¶ 66–82.

[31] The DPD, *supra* note 28, at art. 12(b).

[32] *Id.* at art. 14(a).

[33] C-131/12 *Google Spain SL*, ¶¶ 66–82.

were entitled to erasure where appropriate, and that they have a right to object to certain types of processing.[34] It makes considerable sense that the former should follow from the latter as, if the data were not erased, an objection would become effectively meaningless. However, Articles 14 and 12 both contained significant wiggle room for interpretation. For example, Article 14(a) required a "justified objection" and Article 12(b) only permitted erasure where "appropriate."[35] It is therefore not surprising that the ECJ spent several paragraphs emphasizing that such erasure requests must involve a weighing up of the various competing interests, including the freedom of expression and information.[36] Equally, nobody will have been shocked that soft-law guidance was issued by the Article 29 Working Party[37] as to the implementation of the decision which attempted to offer aid for controllers who were confused by the ambiguities arising from the decision.[38] Fortunately, given the differences between the GDPR and the right as described by *Google Spain*, it is not necessary to go into the impacts of these uncertainties—rather, it is sufficient to note the contrast between the two implementations and to bear in mind the potential implications of the fact that the right to erasure is now considerably more specific and specified.

2. Article 17(1)(b)–(e): Unlawful Processing and Erasure as Remedy

Returning to the GDPR, it is important to examine the individual grounds for erasure before considering the potential impact on the freedom of expression and information. Of the grounds, five of the sub-paragraphs in Article 17(1), specifically (a)–(e), relate either

---

[34] The DPD, *supra* note 28, at arts. 12(b), 14(a).

[35] *Id.* at arts. 12(b), 14(a).

[36] C-131/12 *Google Spain SL*, ¶¶ 80–87.

[37] The Article 29 Working Party was an EU-wide body made up of, *inter alia*, representatives from the Data Protection Authorities of each Member State that offered authoritative soft-law interpretations, guidance and opinions on data protection issues. The DPD, *supra* note 28, at art. 29. The body has now been replaced by the European Data Protection Board, which is governed under the GDPR, Chapter VII, Section 3.

[38] ARTICLE 29 WORKING PARTY, GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON "GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/121, WP225 *passim* (2014).

directly or indirectly to illegal or unlawful processing. Consequently, erasure in such cases should not be considered as an independent concept on its own, but rather as an effective remedy to stop the unlawful processing. This position is similar to the spirit of the DPD, Article 12(b), with the added advantage that most of the grounds under the GDPR, Article 17(1)(a)–(e) are considerably clearer; rather than a general concept of erasure where "appropriate," each situation seemingly already represents the result of a balancing act between the rights of data protection and freedom of expression and information as performed by the EU legislature.

Of these grounds, the easiest to examine are (b)–(e). Before doing so, it is worth noting that the GDPR sets out a closed list of justifications for the processing of personal data under Article 6 (for most types of personal data) and Article 9 (for special category personal data, such as health data or information relating to one's political or religious views).[39] As a result, a controller can only store that data if they have a legally accepted reason under Article 6 (for non-special category data) or Article 9 (for special category data).[40] Given this, it is not surprising that sub-paragraphs (b) and (c) provide the ability for a data subject to demand erasure if no such ground exists.[41] Equally, sub-paragraph (d) allows for erasure if the data is "unlawfully processed" and, as storing data is considered a form of processing under the GDPR, it makes little sense that a controller would be able to continue storing the data in such circumstances.[42] Finally, sub-paragraph (e) applies where retention of the personal data would be contrary to an EU or Member State law other than the GDPR; under such a case, the same consideration (i.e., that retention of the data is unlawful, and therefore the controller has no business retaining it) would apply.[43] Under each of these circumstances, the right to erasure, in many ways, operates not as an independent right but almost as a *de facto* "remedy" for correcting unlawful processing activities.

---

[39] The GDPR, *supra* note 2, at arts. 6(1), 9(1)–(2).
[40] *Id.* at arts. 6(1), 9(1)–(2).
[41] *Id.* at art. 17(1)(b)–(c).
[42] *Id.* at art. 17(d).
[43] *Id.* at art. 17(e).

How, then, do these grounds interact with the freedom of expression and information? Once the premise that the processing of personal data is something that is governed by law has been accepted, it must presumably also be accepted that, as part of this, the law must make it unlawful to possess and process personal data under certain circumstances. Where this has happened, it further makes sense that data subjects should have the right to demand that data that is unlawfully held is erased, or else such conditions become effectively meaningless.[44] In such cases, where the processing is clearly unlawful, there may be little room for a case-by-case balancing between the protection of personal data and the freedom of expression of information. While one may argue that, e.g., the storing of personal data should be permitted even if there is no lawful justification under Article 6, the question would not be whether the erasure in this particular case violates the freedom of expression and information, but whether the general prohibition on an unlawful nature of processing in such conditions violates that freedom in the first place.

Importantly, even at this early stage, it is possible to see signs of regional variance in the right to erasure. In particular, the GDPR, Article 17(1)(e) allows for a slightly wider variation than the other grounds discussed already as it can be used to require erasure on the basis of laws passed by Member States.[45] In all other instances, the balancing act of fundamental rights is being performed by the EU legislature but, where the law being used to justify the erasure is

[44] One could, it is accepted, argue that the right to demand erasure is not strictly speaking necessary and that instead the controller should be subject to damages, with continued damages being available if the data continues to be unlawfully processed. Equally, one could argue that the data subject's direct intervention is not necessary at all and that the situation is better dealt with by a regulatory or supervisory authority, with data subjects merely filing a complaint or report, with fines or other penalties being issued for continued processing. However, without getting too philosophical about the various regulatory approaches, this can be seen as simply a technicality and whatever the mechanism, the end result is the same: that if law is to regulate the processing of personal data then there must be circumstances where it expects the controller to delete the data and will take steps to make this happen, whether directly through an erasure order or indirectly through continued fines until the desired outcome is reached.

[45] The GDPR, *supra* note 2, at art. 17(1)(e).

passed by a national legislature, then this will not be possible. Rather, it is presumably for the national legislature to consider the possible impacts and balance the relevant rights. While this has the same effect of depriving courts and enforcement agencies of any discretion to apply Article 17(3)(a) in particular cases, one can easily imagine a situation where a court in one Member State is obliged to erase information, whereas a court in another is not. Notably, in addition to the idea that different Member States may reach different conclusions on the balancing test, Article 17(1)(e) is limited to situations where the controller "is subject" to the legal obligation, meaning that this provision presumably cannot justify application in Member States where that national law does not apply.

3. Article 17(1)(a) and (f): Introducing Judicial Discretion

While also technically dealing with unlawful processing, sub-paragraph (a) does not necessarily fit into the same paradigm as grounds (b)–(e). As the primary balancing test for these cases is determined at a legislative level, they involve comparatively simple questions at the enforcement level—is there still a legal ground for processing, does a law require that data to be deleted, etc.? By contrast, sub-paragraph (a) asks whether personal data is still "necessary" for its original purposes.[46]

As with the grounds previously discussed, this provision acts as an enforcement or effective remedy for other legal provisions. In particular, it seems to best reflect the data processing principles contained in Article 5(1), which states, *inter alia*, that:

> Personal data shall be:
>
> . . .
>
> (b) collected for specified, explicit and legitimate purposes and not further processing in a manner that is incompatible with those purposes . . . ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate,

[46] *Id.* at art. 17(1)(a).

> having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data are processed . . . ('storage limitation') . . .[47]

These principles seem quite vague. However, Article 5(2) states that controllers are "responsible for, and [must] be able to demonstrate compliance with" these rules (the principle of accountability).[48] Further, Article 83 places violations of Article 5 in the higher of the two possible bands for administrative fines.[49] The principle of accountability, the level of fines, and the fact that failure to comply with these principles may lead to a successful erasure request indicate that, although potentially vague, controllers must take the data processing principles as a serious legal obligation.

Given the existence of these principles and the utility of erasure as a way for data subjects to correct their violations then, as with the grounds discussed above, the application of the right to erasure can arguably be effectively operating as a remedy. Nevertheless, use of "necessary" as the limiting factor seems to add significantly more room for debate than under grounds (b)–(e), which function as relatively simple "yes or no" cases. This ambiguity is enhanced by the fact that the necessity is judged against the original purposes for processing the personal data, which will be extremely fact dependent and may itself also raise issues of ambiguity.

This issue of determining what is necessary has already raised interesting issues in case law, albeit in a different form. One example is the case from the High Court of England and Wales in *NT1*,[50] where the Court was asked to remove search engine links which related to past criminal convictions. The case involved two separate claimants, one of whom (NT2) was granted erasure, while erasure

---

[47] *Id.* at art. 5(1).

[48] *Id.* at art. 5.

[49] The GDPR has two bands for fines, the higher capped at €20 million or four percent of total worldwide annual turnover from the preceding financial year (whichever is higher), and the lower at €10 million or two percent of the same. *Id.* at art. 83.

[50] *NT1 v Google LLC* [2018] EWHC 799 (QB) (Eng. & Wales).

was denied to the other (NT1).[51] In relation to NT2's case, Justice Warby found that NT2 had "frankly acknowledged his guilt, and expressed genuine remorse," that his conviction was spent, that "[t]here is no evidence of any risk of repetition" (in part because he had changed fields), and that "[h]is past offending is of little if any relevance to anybody's assessment of his suitability to engage in relevant business activity now, or in the future," and concluded that "[t]here is no real need for anybody to be warned about that activity" and ordered erasure of the information.[52] By contrast, Justice Warby said of NT1 that the information "has not been shown to be inaccurate in any material way," that while his conviction was historic, it was "of such a length" that the claimant had "no reasonable expectation that his conviction would ever be spent," and that "[h]e has not accepted his guilt, has misled the public and this court, and shows no remorse over any of these matters."[53] Justice Warby also noted that "[h]e remains in business, and the information serves the purpose of minimising the risk that he will continue to mislead, as he has in the past," and concluded that the case for erasure was "not made out."[54]

While this case was decided under the DPD as implemented into UK law by the Data Protection Act 1998,[55] clear parallels to the GDPR, Article 17(1)(a) can be seen. One of the primary focuses of the court, as illustrated by the quotations above, was whether the data represented the claimant as they were at the time of the erasure request—or, in other words, whether the information was still necessary for the purposes of informing a reader about the claimant and warning the public about their criminal behavior.[56] This question will inescapably involve an on-the-spot evaluation of data protection rights against the freedom of expression and information; how could one either evaluate the purpose of the processing or the necessity of the data for those purposes without involving such questions? Questions which exist under Article 17(1)(a), then, seem much more

[51] *Id*. ¶¶ 229, 230.
[52] *Id*. ¶ 223.
[53] *Id*. ¶ 170.
[54] *Id*.
[55] Data Protection Act 1998, c.29 (Eng. and Wales).
[56] *See*, *inter alia*, *NT1 v Google LLC*, ¶¶ 170, 223, 227.

likely to require a judge to actively engage the freedom of expression and information under Article 17(3)(a) (or, at least, seem to be much more likely to be capable of doing so). Further, one can at this stage wonder whether the exact way this balancing act plays out could vary from one Member State to another. As will be explored later, one may be able to imagine situations where the strengths of the Charter rights involved vary between countries and, therefore, suggest that Article 17(1)(a) should win in some locations and Article 17(3)(a) in others.

The final ground for erasure is sub-paragraph (f), where the data has been collected in connection with the GDPR, Article 8(1).[57] Article 8(1) itself is engaged if personal data (a) relates to a child under the age of sixteen (although Member States may further lower this age to a minimum of thirteen); (b) was processed on the basis of consent under Article 6(1)(a); and (c) was processed "in relation to the offer of information society services directly to a child."[58] Where these conditions apply, Article 8 states that the initial processing is unlawful unless the consent is "given or authorised by the holder of parental responsibility over the child."[59]

Where personal data relating to a child is processed in such a context and such consent is not given, the processing would be unlawful, and the data could be erased under Article 17(1)(d), even without a dedicated special ground.[60] The extra added value of Article 17(1)(f) is therefore that the data subject (whether or not they are still a child) still has the right to have information erased where the processing of the data was legally performed, whether or not they have formally removed their consent to the processing, and whether or not the controller may have another legitimate basis for processing that data.[61] There are clear normative arguments in favor of this; for example, an adult may, in hindsight, realize that they

---

[57] The GDPR, *supra* note 2, at art. 8(1).

[58] *Id.*

[59] *Id.*

[60] It should be remembered that if a data subject removes their consent, they would normally have a right to have the data erased under art. 17(1)(b) unless the controller had another justification for retaining that data, whether or not they are a child.

[61] The GDPR, *supra* note 2, at art. 17(1)(f).

should not have shared something online, and the law gives greater leeway for correcting that mistake than it would in other conditions. Equally, however, this also seems to be a clear situation where a controller may have a legitimate wish to refuse erasure; the processing was not, and is not now, illegal, and they may well have legitimate reasons to continue processing it, including the freedom of expression and information. Here, then, there is clear scope for the balancing of rights, particularly based on the exception in Article 17(3)(a).

This question becomes even more difficult as its exact implementation may vary from Member State to Member State as Article 8(1) allows Member States to "provide by law for a lower age for [the application of Article 8(1)] provided that such lower age is not below 13 years."[62] It may, therefore, be the case that a data subject between the ages of thirteen and sixteen from one Member State may be able to invoke erasure under Article 17(1)(f), where a data subject of the same age from another Member State may not. There has yet to be decisive case law on whether this rule should be decided based on the location of the data subject, the location of the controller, or some variation of the two.

Both of these grounds, then, introduce more ambiguity and, in particular, begin to provide some leeway for a case-by-case analysis of the extent to which erasure may affect the freedom to expression and information. Importantly, and as will be explored later, these case-by-case analyses may have a geographical consideration, with the balance tipping one way or another depending on the different countries involved.

4. Data Protection, Journalistic Truth and Reconciliation Across Borders: Article 85 and Beyond

Article 8 is not the only provision which provides explicit grounds for geographical variations. As noted above, Article 85 requires that:

> (1) Member States shall by 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

[62] *Id.* at art. 8(1).

> purposes and the purposes of academic, artistic or literary expression.
>
> (2) For processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles [which contains Articles 5, 6 and 9], Chapter III (rights of the data subject) [which contains Article 17] [as well as Chapters 4, 5, 6, 7 and 9] . . . if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.
>
> (3) Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 . . .[63]

This is an extremely interesting provision which provides much fuel for discussion. In particular, the interaction between Article 85 and Article 17(3)(a) is interesting given the overlapping subject-matter of the two provisions and, while Article 17(3)(a) may not automatically seem to create a regional variation for erasure, the combination with Article 85 raises at least the possibility that the true case may be otherwise.

As a starting point, the discretion provided in Article 85 feels a little odd. Being a regulation, the GDPR's rules are directly binding on Member States[64] and, as Member States are not entitled to independently interpret EU law,[65] individual countries must follow a central concept of both the right to the protection of personal data, and the Charter right to the freedom of expression and information. Particularly important for the purposes of Article 85, this lack of competence to interpret EU law means that Member States are not able to independently interpret how much discretion they are given by the term "reconcile" in Article 85. Nevertheless, Member States may have their own constitutional conceptions of the freedom of expression and information, or of concepts of privacy and data

---

[63] *Id.* at art. 85.

[64] TFEU, *supra* note 19, at art. 288. This is generally opposed to Directives, which must be implemented into national law and therefore leave more scope for national variation, particularly as to the "form and methods" of implementation. *Id*.

[65] *See, e.g.*, the TFEU, *supra* note 19, at art. 267; Case 6/64 *Costa v E.N.E.L*, 1964 ECR 01141; ECLI:EU:C:1964:66; and Case 11/70, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, 1970 ECR 01125; ECLI:EU:C:1970:114.

protection, which may need to be resolved under the Article 85 procedure.[66] Further, as will be discussed in more detail below, EU law must be drafted in line with a certain number of principles. This includes the principle of subsidiarity, which states that if the Treaties do not give the EU exclusive competence in an area, it should only act if "the objectives of the proposed action cannot be sufficiently achieved by the Member States . . . but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level."[67] Article 85 plays an important role in this regard, allowing Member States to protect the freedom of expression and information in a way which complies with this principle.[68]

Within the discretion granted to Member States by Article 85, there are two interesting differences between paragraphs (1) and (2). Of the two, paragraph (1) is more general, but weaker, covering the entirety of the GDPR and the freedom of expression and information in general but only requiring a reconciliation of rights.[69] By contrast, paragraph (2) is more powerful, but narrower, allowing Member States to "provide for exemptions or derogations" but only covering specific parts of the GDPR and only applying for processing that is performed for specific purposes.[70] One would be forgiven for wondering how a Member State should reconcile the rights of data protection and the freedom of expression and information under paragraph (1) if it is not able to suspend or exempt GDPR rules, particularly given the interpretive restrictions

[66] It is perhaps interesting to note in this context that, despite early conversations on the topic, fundamental rights did not gain any notable legal protection under EU law until the ECJ was directly confronted by incompatibilities between EU law and German constitutional rules. *See, e.g.*, Case 11/70, *Internationale Handelsgesellschaft*. Fundamental rights in the European Union can, therefore, be seen in some way as a way of allowing Member States to protect human rights while maintaining the supremacy of EU law. For an interesting discussion on the history of fundamental rights in the European Union see, for example, Gráinne De Búrca, *The Evolution of EU Human Rights Law*, in THE EVOLUTION OF EU LAW (Paul Craig and Gráinne De Búrca eds., 2nd ed. 2011).

[67] TFEU, *supra* note 19, at art. 5(3).

[68] The GDPR, *supra* note 2, at art. 85.

[69] *Id.*

[70] *Id.*

discussed above. Equally, it seems odd that paragraph (2) is so limited to journalistic, academic, artistic, and literary expressions as this selection feels somewhat arbitrary. In many ways, one is therefore left to wonder what the practical effect of each of these provisions was intended to be, will be, and why the two were separated in this way.

Regardless of how exactly Member States choose to implement Article 85, the core message is the same: that the GDPR accepts, and moreover endorses, that certain provisions must play out differently in different Member States. This is interesting for erasure, as Article 17 is included in the provisions which can be exempted under Article 85(2).[71] One can, therefore, easily imagine a situation where such an order is permitted (or even required) in one Member State, but not in another. Presumably, this would require that the erasure be ordered on a geographically limited basis between Member States. Given that this variation is based on the fact that different Member States may need to act in different ways to protect the freedom of expression and information, this must therefore be taken as more evidence of the GDPR's acceptance that geographical considerations will affect the balancing of the protection of personal data and the freedom of expression and information.

Having established these different grounds for variations, it is interesting to quickly look at the law's claims to harmonization.[72] In particular, it may be very easy to overstate the aims and effects of the law in this field. In Recital 7, the GDPR does not say that unified rules must be implemented, rather that there is a need for "a strong and more coherent data protection framework."[73] Further, Recital 9 criticizes the fragmentation causes "differences in the *level* of protection," not that fragmentation provides differences in the implementation of that protection per se.[74] In theory, therefore, arguably the harmonizing aims of the GDPR do not necessarily aim for the same practical rules, or even the same results or conclusions,

---

[71] The GDPR, *supra* note 2, at art. 85(2).
[72] *See, e.g.*, *id.* at Recitals 3–7.
[73] *Id.* at Recital 7.
[74] *Id.* at Recital 9 (emphasis added).

as so much that it aims for the same frameworks and levels. This idea would be supported by the discussion above and the idea that the GDPR recognizes that, inevitably, the rights can only be properly balanced when geography is considered. Nevertheless, if this produces different substantive rules or ends up with notably different results from one Member State to another, it is questionable how useful a unified framework would be for either data subjects or controllers. At the very least, the text of the law seems to suggest that perhaps perceptions of the GDPR as a monolithic, homogenous set of data protection rules across the European Union deserve reconsideration.

B. Google LLC v. CNIL*: What Actually Happened?*

The potential for regional variation in erasure requests discussed above is not simply hypothetical, or simply based on a reading of the GDPR. Rather, this very issue was discussed by the ECJ in the case of *Google LLC v. CNIL*.[75] This Section will examine that case, its context, and the decision of the ECJ to draw some conclusions about the way that the Court sees geographical variations in the right to erasure.

1. Going Courting

Google LLC v. CNIL began life as a decision by the CNIL ordering that, when Google grants an erasure request, it must delete the search results from each instance of its website, to take effect regardless of the country from which the search was made.[76] Google rejected this decision, instead only deleting results from searches made within the European Union.[77] The CNIL subsequently issued a fine against Google, which in turn sought annulment of the decision with the French court, the *Conseil d'État*.[78] That court determined that the decision involved the interpretation of EU law and therefore made a preliminary reference to the ECJ.[79]

---

[75] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019) (judgment).

[76] *Google LLC v. CNIL* (judgment), ¶ 30.

[77] *Id.* ¶ 31.

[78] *Id.* ¶¶ 33–34.

[79] *Id.* ¶¶ 30–39.

It may be useful at this stage to make two points about the preliminary reference procedure.[80] First, as was already noted, national courts have no jurisdiction to interpret points of EU law and must refer such questions to the ECJ.[81] The other side of this is that the ECJ has no jurisdiction to interpret national law and cannot decide issues of fact.[82] As a result, the ECJ did not make a final decision in the case, which was returned to the *Conseil d'État* for final adjudication.[83] Secondly, while the European Union does not follow a common law system, for the purposes of this Article, the ECJ's rulings can be effectively seen as setting precedents[84] and, absent either legislation or the ECJ deciding to answer another preliminary reference, *Google LLC v. CNIL* can be seen as representing the state of the law. However, it is important to note that there are no rules concerning which parts of the ruling is actually binding. Further, as was arguably best described by Craig and de Búrca:

> The ECJ's . . . judgments are collegiate, representing the single ruling of all judges hearing the case. There are no dissents or separately concurring judgments, and therefore divergent judicial views may be contained within the judgment. This can result in a ruling that is ambiguous on matters of importance . . . Moreover . . . the Court may

---

[80] For more information on the functioning of the ECJ, see, e.g., PAUL CRAIG, EU ADMINISTRATIVE LAW, Chapter 10, 261–88 (2nd ed. 2012).

[81] *Id.*

[82] *See* Information Note on References from National Courts for a Preliminary Ruling, 2005 O.J. (C 143) 1, ¶ 5.

[83] This was done in *Conseil d'État* 27 Mars 2020, N 399922. Readers wishing to avoid spoilers as to how the story ends may wish to skip the rest of this footnote. For those who remain, the French Court annulled the fine in light of the ECJ's decision.

[84] The ECJ has previously stated that while answers to preliminary references are given to the referring court, courts from other Member States can rely on that decision for the interpretation of EU law. However, national courts must still make a preliminary reference if they think that the new case is sufficiently different that a question must be raised again. *See*, *e.g.*, C-66/80 *International Chemical Corporation v Amministrazione delle finanze dello Stato*, 1981 ECR 01191; ECLI:EU:C:1981:102, ¶¶ 13–14. While courts are entitled to bring preliminary references even where no new ground is covered, the ECJ is likely to simply refer to the previous decision. *See*, *e.g.*, Joined Cases C-28–30/62 *Da Costa en Schaake NV, Jacob Meijer NV, Hoechst-Holland NV v Netherlands Inland Revenue Administration*, 1963 ECR 00061; ECLI:EU:C:1963:6, ¶¶ 38–39.

> prefer not to commit itself on a specific legal issue until another case arises where it is directly necessary for a decision.[85]

Having provided this background, it is now possible to return to *Google LLC v. CNIL*. In that case, the French court referred three questions to the ECJ, asking:

> (a) whether a search engine could be ordered to erase (or, in the language of the question, de-reference) search results globally;
>
> (b) if not, whether, a search engine granting erasure must remove the results in all Member States or just the place where the request was made; and
>
> (c) whether a search engine is obliged to use geoblocking techniques to prevent users in places where erasure was made from finding the results via another location's version of the search engine.[86]

In answering these questions, which were "dealt with together,"[87] the ECJ framed its decision "in light of both [the DPD] and [the GDPR] in order to ensure that its answers will be of use to the referring court in any event."[88] On the one hand, this improves the value of the case as precedent as readers can be certain that its effectiveness shall continue under the new regime. On the other hand, dealing with such a wide variety of issues and sources at once does make it harder to derive specific points of utility (especially where the decision matches the style described by Craig and de Búrca).[89]

To begin with the conclusion, the ECJ gave the following answers to the French court's questions:

> (a) "[C]urrently, there is no obligation under EU law . . . for a search engine operator to carry out such a de-referencing on all versions of its search engine" and the GDPR,

---

[85] PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW: TEXT, CASES AND MATERIALS, 63 (5th ed. 2011).

[86] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶ 39 (Sept. 24, 2019) (judgment).

[87] *Id*. ¶ 43.

[88] *Id*. ¶ 41.

[89] CRAIG & DE BÚRCA, *supra* note 85.

Article 17 cannot be read as requiring a controller do to so.[90] However, EU law "does not prohibit such a practice" if, after balancing the rights of privacy, data protection, and freedom of expression and information, such an order is "appropriate";[91]

(b) While, "in principle," erasure is "supposed to" occur in all Member States, "the interest of the public in accessing information may, even within the Union, vary from one Member State to another" such that the balancing of rights may require different answers in different countries. Where processing occurs across multiple Member States, it is for national Data Protection Authorities to "reach a consensus and a single decision" as to the extent of the erasure requirements;[92] and

(c) Search engines must take "sufficiently effective measures to ensure the effective protection" of fundamental rights and it is up to the national court to determine what measures are required.[93]

There is a lot to unpack from this judgment and, in many ways, one could say that it seems to raise more questions than it actually answers. However, a key takeaway from the passages above is that, under EU law, the right to erasure can be subject to geographical limitations, and one of the key factors when determining these limitations is the balancing of interests between the right to the protection of personal data and the right to the freedom of expression and information.[94] This conclusion supports some of the conclusions and themes suggested in Section II.A above, but also inherits some of the difficulties raised there. Indeed, the idea of location-based erasure, while sensible in some regards, is conceptually difficult and inconsistent in others—particularly when that balance is based on a

[90] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶¶ 64–65 (Sept. 24, 2019) (judgment).
[91] *Id*. ¶ 72.
[92] *Id*. ¶¶ 66–69.
[93] *Id*. ¶ 70–71.
[94] *Id.* ¶¶ 64–72.

supposedly harmonizing regime and EU-wide concepts of fundamental rights.

Before beginning a deeper analysis of *Google LLC v. CNIL*, it is important to consider the scope of the judgment. The Court in that case focused on the term "dereferencing" rather than "erasure" and framed its discussion clearly in terms of search engines.[95] This is, in part, because of the nature of the case; as a preliminary reference, the ECJ is answering the question put to it, which involved a search engine and was phrased by the French court in terms of a right to dereferencing.[96] Nevertheless, it would be a mistake to assume that the decision cannot be extended to other types of controllers. First, the GDPR, Article 17 does not contain any language that would limit itself in such a way and is rather framed against controllers as a whole, which means that erasure is enforceable against any controller.[97] Secondly, while conceivably there may be controllers to whom the considerations discussed in *Google LLC v. CNIL* may or should not apply, nothing suggests that search engine operators are sufficiently unique that the judgment must be narrowed so particularly.

2. There Is No Right to a Global Erasure (At Least for Now . . .)

The first major point of analysis will be the differences between its treatment of intra- and extra-EU processing. In reaching its finding on this point, the ECJ relied on a number of factors. During its analysis, the Court noted that the purpose of the GDPR was to "guarantee a high level of protection . . . throughout the [European Union]"; that global erasure "would meet that objective in full";[98] and that "in a globalised world," access by users (whether inside or outside of the European Union) to personal data online was "likely to have immediate and substantial effects on that person."[99] These considerations, the Court claimed, would have justified the EU's legislature to create a global right to erasure.[100]

---

[95] *Id.* ¶¶ 39–73.
[96] *Id.* ¶ 39.
[97] The GDPR, *supra* note 2, at art. 17.
[98] *Google LLC v. CNIL* (judgment), ¶¶ 54–55.
[99] *Id*. ¶ 57.
[100] *Id*. ¶ 58.

However, the ECJ further noted that not all countries recognized a right to erasure (and that, if they did, they did not do so in the same way),[101] and the right to data protection must be balanced against other rights, including the freedom of expression and information—a balance which was "likely to vary significantly around the world."[102] The ECJ placed a heavy emphasis on the actual wording of Article 17, stating that it was "in no way apparent" that the Article was intended to create a global scope of application.[103] The Court further stated that Article 17(3)(a) showed that the EU legislature had "struck a balance between [the right of data protection] and the [freedom of expression and information] so far as the Union is concerned . . . [but] it has not, to date, struck such a balance as regards the scope of [erasure] outside the Union."[104]

Based on this analysis, the Court concluded that Article 17 did not create a global obligation for erasure.[105] This decision is interesting for a number of reasons. Notably, the ECJ did not discuss the impact of Article 3 of the GDPR (which governs the territorial scope of the GDPR).[106] This omission seems slightly odd as, prima facie, Article 3(2)—which states that certain processing activities outside of the EU still fall within the scope of the GDPR—would seem to be a controlling provision. Nevertheless, from a practical and political position, one can understand why the ECJ would be less than willing to demand a global erasure that would be difficult, if not impossible, to enforce.

Equally interesting is that the Advocate General[107] also somewhat sidestepped the issue represented by the GDPR, Article 3.

---

[101] *Id.* ¶ 59.
[102] *Id.* ¶ 60.
[103] *Id.* ¶ 62.
[104] *Id.* ¶ 61.
[105] *Id.* ¶ 64.
[106] The GDPR, *supra* note 2, at art. 3.
[107] Advocates General are members of the ECJ which provide an impartial Opinion to the Court. TFEU, *supra* note 19, at art. 252. The Opinion is given by one of the Advocates General as part of the oral submissions for a case, although the ECJ can skip this if the case does not raise a novel point of law. TFEU, *supra* note 19, at Protocol (No 3) on the Statute of the Court of Justice of the European Union, art. 20. Importantly, despite the Advocate General being a member of the ECJ and while their Opinions can often be described as persuasive, there is no law

In his Opinion, A.G. Szpunar first stated that while the French court's questions asked about both the interpretation of the GDPR and the DPD, "there can be no doubt" that the DPD was the controlling law of the case and therefore the ECJ was not required to interpret the terms of the GDPR.[108] He then analyzed the applicability of the law, not on its provisions, but on the general principles of extraterritoriality and found that EU law could not apply outside of its borders unless exceptional circumstances applied, none of which applied here.[109] Having reached this conclusion, A.G. Szpunar considered whether the fact that data protection was a fundamental right could change this result. He observed that as "the scope of the Charter follows the scope of EU law and not vice versa"[110] and that, if worldwide erasure were permitted, it would become impossible to balance the right of data protection with the freedom of information and expression because the latter "will necessarily vary, depending on its geographic location, from one third State to another."[111] He further argued that, if the European Union were to impose a global erasure right, this may encourage third countries to create their own erasure laws, which could cause "a genuine risk of a race to the bottom, to the detriment of freedom of expression."[112]

A key element in both the Court's judgment and the Advocate General's Opinion is that, while both went through different mechanisms to get there, both focused on the balancing of rights and relied on the idea that geographical location could alter the importance of certain information or data. However, interestingly, both the ECJ and the Advocate General seemed to take this conclusion for granted—or, at least, did not go into detail explaining why this may be the case.

---

to say that the ECJ is bound to follow the Opinion, either in structure or substance (as seen occurring in this case).

[108] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:15, ¶ 32 (Jan. 10, 2019) (op. of advoc. gen.).

[109] *Id.* ¶¶ 47–53.

[110] *Id.* ¶ 55.

[111] *Id.* ¶ 60.

[112] *Id.* ¶ 61.

Certainly, it is possible to imagine some situations where information may be more important in one area than in another. For example, information that changes whether voters want to elect a particular candidate in the Dawlish Town Council election may be important for the 11,662 people eligible to vote in that area.[113] However, for the 446 million inhabitants of the European Union,[114] or 7.8 billion people in the world,[115] that information would undoubtedly have little, if any, importance or relevance. Nevertheless, one should be careful treating the issue as such an open and shut question. Once the discussion leaves behind questions involving the voting booth, things quickly get much more complicated, and the answers to the questions quickly become much more subjective. Why, for example, is news about a certain celebrity more important in one region than another? How popular does a businessperson's products have to be before their scandal becomes relevant to a particular region? What geographical lines can be drawn around the relative importance of crime? Even within politics, it is very hard to provide arguments for why speech may be more important in one area than another; while only American citizens can vote for the President of the United States, information about U.S. elections and the behavior of candidates can be important and influential news throughout the world.

In a way, the questions raised here are slightly unfair as they are, by and large, unanswerable (at least to any satisfactory legal standard). Further, the issues raised by these questions actually support the ECJ's conclusion—given the difficulty in balancing the protection of personal data and the freedom of expression and information, particularly in a global context, it would be wrong to claim that the GDPR, Article 17 was an appropriate tool to regulate the issue. Nevertheless, it would have been preferable for the Court to engage a little more openly with the issue, rather than simply relying on the vague and unsupported assumption of self-evidence.

---

[113] Teignbridge District Council, Electoral Roll (2020).

[114] *Living in the EU*, EUR. UNION, https://europa.eu/european-union/about-eu/figures/living_en) [https://perma.cc/35WU-A5JV] (accessed May 14, 2020).

[115] *Current World Population*, WORLDOMETER, https://www.worldometers.info/world-population/ (last visited May 14, 2020) [https://perma.cc/496H-C5W6].

This greater engagement would also have helped with the fact that, confusingly, neither the Advocate General nor the ECJ finished with a simple dismissal of global erasure. Almost as an afterthought (in a single paragraph at the end of its judgment, which tellingly begins "Lastly,"), the ECJ added that while EU law did not "currently require" global erasure, it also did not "prohibit" it where the balancing of rights required such an order.[116] For his part, A.G. Szpunar added a final paragraph to his analysis stating that he did "not exclude the possibility that there may be situations" where EU law could require worldwide erasure.[117]

These comments leave a number of unanswered questions at the end of the judgment. While the Advocate General was clear that the DPD could not support a global erasure order, and that new EU legislation would be required for such an order to be possible, he did not comment on whether the GDPR had imposed such a rule.[118] This is particularly notable given that the GDPR contains new rules on territorial applicability under Article 3, which were not substantively addressed by either the Opinion or the Court's judgment. Meanwhile, the ECJ seemed to leave it open to "a supervisory or judicial authority of a Member State" to decide that a global order would be appropriate "in light of national standards of protection of fundamental rights."[119] While this may seem like a convenient loophole, the ECJ also found that Article 17 did not create such a power and, as the ECJ is the only body capable of interpreting the GDPR and Member States are therefore very limited in their powers to legislate around that law,[120] one may wonder under what legal basis such an order could actually be made. In many ways, this paragraph may seem to imply that the ECJ has simply

---

[116] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶ 72 (Sept. 24, 2019) (judgment).

[117] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:15, ¶ 62 (Jan. 10, 2019) (op. of advoc. gen.).

[118] *Id*. ¶¶ 47–63.

[119] *Google LLC v. CNIL* (judgment), ¶ 72.

[120] *See* The TFEU, *supra* note 19, at art. 267; Case 6/64 *Costa v E.N.E.L*, 1964 ECR 01141; ECLI:EU:C:1964:66; and Case 11/70, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, 1970 ECR 01125; ECLI:EU:C:1970:114.

reserved the right to change its mind in the future; for now, Article 17 does not impose a global erasure regime, but it may do so in the future.

3. EU-Based Erasure: A Little Respect

The next element of the decision for consideration is the ECJ's finding that an erasure order does not necessarily have to cover the entirety of the European Union, provided that the erasure occurs in the geographical locations necessary to ensure the protection of the data subjects' rights.[121]

The Court did not give this issue as much consideration as the idea of global erasure, although it implicitly relied on very similar logic. As before, the ECJ began by noting that global erasure was "in principle" necessary to meet the GDPR's goals,[122] but that the interests in accessing information may be different in different Member States, and that this may change the balancing of rights, "in particular" where processing relates solely to journalistic purposes, or artistic or literary expression, and so fall under Article 85(2).[123] The solution provided by the Court was that this question be dealt with by national Data Protection Authorities (being the national bodies empowered by the GDPR, Chapter VI to deal with issues of data protection compliance and enforcement), which can use the various cooperation and consistency mechanisms to "provide each other with relevant information and mutual assistance" and "reach a consensus and a single decision."[124] It is, the Court concluded, up to these Authorities to decide whether an EU-wide erasure order was necessary, or (implicitly) whether the data subject's rights could be appropriately protected and balanced against the freedom of expression and information with a more restricted order.[125]

This discussion mirrors a lot of the above debate as to global erasure. However, there is one important difference—unlike global erasure, where there are live questions as to the applicability and enforceability of the GDPR, erasure requests in the European Union

---

[121] *Google LLC v. CNIL* (judgment), ¶ 69.
[122] *Id*. ¶ 66.
[123] *Id.* ¶ 67.
[124] *Id*. ¶ 68.
[125] *See id*. ¶ 69.

are firmly grounded in and enforced under that law. It is, therefore, important to resist the urge to get lost in general and abstract discussions about the balancing of rights and stay firmly focused within Article 17 itself. As discussed above, questions of local discretion are likely to focus around Article 17(1)(a), (e) and (f), or where Article 17 has been suspended in some way under the Article 85(2) procedure (and, even then, questions involving Articles 17(1)(e) and 85(2) will focus on discretion with the local legislature).

In terms of compliance and enforcement, it is at least conceptually easier to deal with geographical variations under Articles 17(1)(e) and 85. This is because these variations must be set out as established legal rules (e.g., statute), rather than being decided on a case-by-case basis. While there is room to argue about whether or not the particular geographical boundaries are appropriate or justified, they will at least be clear, as they are limited to the jurisdiction of the relevant laws. It is also likely that cases involving journalistic, literary, or artistic expressions may feature some of the more important (or, at least, dramatic and high-profile) balancing issues. Certainly, such cases seemed to draw a focus in the ECJ's analysis, although notably, in the decision of *Google Spain*, the ECJ focused on Google's economic interests in displaying search results, rather than its journalistic role.[126] In addition to this, it must be remembered that Article 85 only applies where decisions are "solely" for the specified purposes, which is a significant narrowing of the exception.[127]

Such cases, then, are comparatively easy; the geographical limitations will largely be set out by law and the question will (in ideal cases) be resolved by a comparison of the various statute books. By contrast, cases where erasure is requested because the data is no longer necessary under Article 17(1)(a) or because the information relates to a child and was processed in the context of an information society service on the basis of consent under

---

[126] *See* Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD)* (C-131/12 *Google Spain SL*), ECLI:EU:C:2014:317, ¶ 81 (May 13, 2014).

[127] The GDPR, *supra* note 2, at art. 85.

Article 17(1)(e) contain open questions about the amount of scope that actually exists for regional variations.

To first examine a situation of necessity, the following hypothetical is useful. For example, one can imagine a system created to provide a list of individuals who offer certain services. This list is not created for advertising purposes, but as a form of expression, e.g., because the list operator's political beliefs mean that they wish to praise or to condemn actors in a certain field. A service provider who had previously acted in three countries and who is included in the list ceases to act altogether in country A, ceases to offer the specific service but remains active in the field generally in country B, and continues to offer the original service in country C. The processing of the information in question, being the inclusion of the service prover on the list, is no longer necessary for the original purpose in countries A and B, but is still necessary in country C. Prima facie, then, there would be a case for erasure under Article 17(1)(a), at least insofar as relates to countries A and B. The operator may, however, argue that their freedom of expression and information allows them to keep the information available in country A because of the data subject's historic involvement with the service and in country B because of their continued, related activities.

In this example, it is argued that the relevant interests (and the relevant weight of each interest) clearly vary between each country. As a result, the implementation of the balancing act must also be different in each of the three locations, although it is very difficult to say at this level of detail whether it would be different enough to produce different erasure-request results. Regardless of the specific end-result, the fact that situations such as this raise the question means that there is reasonable scope for Member State-specific erasure orders to exist, and it seems reasonable to ask supervisory authorities (using their local knowledge and the cooperation procedures laid out under the GDPR) to address these questions at an enforcement level. However, it must also be emphasized that localized orders would only be a realistic option if they can be reliably enforced—an issue to which this Article will return.

If this possibility is accepted, the ECJ's conclusion therefore seems reasonable, although cases which fit into these scenarios are likely to involve significant room for debate as to what should be the correct outcome. Further, while the facts would clearly be different, it is argued that the same result is at least conceptually possible in cases involving Article 17(1)(e).

Interestingly, however, the Advocate General reached the opposite conclusion to the ECJ on the issue of EU-wide erasure orders.[128] Unlike under the first question, A.G. Szpunar did answer this question by reference to the GDPR, stating that, as a regulation, it "transcends the internal-market approach of [the DPD] . . . to ensure a complete system of personal data protection" and therefore the only answer was that erasure "must be carried out not at a national level . . . but at EU level."[129] This approach would certainly be easier from a compliance point of view, and would certainly help to ensure a strong and consistent protection for personal data rights. However, with respect to the Advocate General, and recognizing that the GDPR is equally applicable in all Member States, the Authors prefer the conclusion reached by the ECJ. In particular, the reasoning given does not seem to have fully considered: that data protection is a qualified (not an absolute) right, the varying importance of the freedom of expression and information from one Member State to another, or the fact that Articles 17(3)(a) and 85(2) permit national variation within the unified GDPR regime.

4. Geoblocking and Other Technological Solutions

The final question addressed by the decision was whether geoblocking, or other equivalent tools, should be used as part of an erasure order.[130] Both the ECJ and the Advocate General dealt very quickly with this question, and neither provided any significant discussion or analysis. The Court simply stated that where an order is made, the controller must "take, if necessary, sufficiently effective

[128] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:15, ¶¶ 75–77 (Jan. 10, 2019) (op. of advoc. gen.).

[129] *Id.*

[130] Case C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶¶ 70–71 (Sept. 24, 2019) (judgment).

measures" to "meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users," and that these measures could be reviewed by national courts.[131] Equally concisely, the Advocate General stated that if an erasure order is made, controllers must take "all the steps which are technically possible" to comply effectively, including geoblocking.[132]

Once one accepts that an erasure order deserves to be made, and if one also accepts that an erasure order does not have to be made globally, the use of geoblocking and other technical tools seems inescapable. An order which could be easily circumvented by simply navigating to a different top-level domain (e.g., swapping from .eu to .com, or from .fr to .fi) would be no true protection at all. Equally, if a controller is ordered to erase the personal data from search results (or equivalent) in a certain jurisdiction, they can hardly be said to have complied with that order if they do not actually take steps to stop that information from being accessible in that region; leaving aside the spirit of the order, it cannot be said to be complying with the letter of such an order if one simply removes the information from the "targeted" version of a website.

However, there are two issues which should be raised at this point. The first is whether the concept of geoblocking changes the normative evaluation of the right to erasure as a whole. Any concept of geoblocking will inevitably give rise to questions about a fragmented internet, the idea that the so-called "world wide web" is no longer such because a person's level of access depends on where they live.[133] This fragmentation is both a conscious and deliberate consequence of the ECJ's judgment, and it must be for the reader to decide whether they consider this a positive or a negative. Ultimately, however, it would seem impossible to properly respect any variations in the balancing of rights without such fragmentation,

---

[131] *Id*.

[132] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:15, ¶ 74 (Jan. 10, 2019) (op. of advoc. gen.).

[133] For a discussion of this issue, see, e.g., Jonathan Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law* (Harv. L. Sch. Pub. L., Research Paper No. 60, 2003).

and, if one decides that it is something to be avoided, one must also decide which of the competing rights must be the one to suffer.

Secondly, the actual efficiency of geoblocking and other technological measures cannot be guaranteed. While they will undoubtedly dissuade some users from accessing information, others may be able to circumvent such limitations. For example, to avoid geoblocking based on the user's IP address, a user could connect through a virtual private network ("VPN"), making it appear as though they are connecting from a different address (specifically one registered to a location that is not blocked).[134] Such a service would allow somebody to appear as though they are connecting from a location in which the data has not been erased, and therefore access the data notwithstanding that it would otherwise be unavailable in their country. It is worth further noting, however, that such services should not be considered a silver bullet to geoblocking techniques; there are other methods of detecting a user's location which may betray the truth notwithstanding measures taken.[135] Further, some websites may simply refuse service if they think that the user is attempting to use a service to conceal their real location.[136]

The ECJ did not seem to engage with these issues, rather leaving it for the Data Protection Authorities to determine what was appropriate or necessary in any particular case. This aspect of the judgment can be criticized, since arguably the question of geoblocking is core to the question of geographical limitations and variations with erasure, at least from a practical perspective. Ultimately, however, this issue seems to be somewhat irrelevant from a theoretical perspective; if the law admits, or even requires,

---

[134] This issue has been much discussed in a variety of fields and academic, professional, or consumer focuses. In law, the use of VPNs is often discussed in relation to accessing copyrighted material that is hidden behind geo-blocks. *See, e.g.*, Sabrina Earle, *The Battle Against Geo-Blocking: The Consumer Strikes Back*, 15 RICH. J. GLOB. L. & BUS. 1, 1 (2016).

[135] *See, e.g.*, *What is a DNS Leak and why Should I Care?*, DNS LEAK TEST.COM, https://www.dnsleaktest.com/what-is-a-dns-leak.html [https://perma.cc/F2ZV-BWRF] (last visited Jan. 30, 2020).

[136] *See, e.g.*, *iPlayer*, BBC, https://www.bbc.co.uk/iplayer [https://perma.cc/68V4-DRLF] (last visited Jan. 30, 2021) (refusing access if the user attempts to connect with an IP address known to be used by VPN services).

geographical variations, as the right to erasure has been shown to do, it must also require some kind of enforcement or else render those measures pointless. Further, if one believes that such measures are necessary, this may be an area where the perfect becomes an enemy of the good, since there is unlikely to be any sudden development or change allowing for a fool-proof and complete geoblocking system.

C. Equal Protection, Different Results?

The above Sections have analyzed both the text of the GDPR and the case of *Google LLC v. CNIL* and found numerous areas where the right of erasure, as balanced against the freedom of expression and information, requires geographical variations, both inside and outside of the European Union. This creates a strange system where, although the rights gain the same protection in each country, that protection may play out to provide different results in different locations.

Importantly, this is not necessarily seen as a criticism of the GDPR. Although the law intended to provide a single regime to cover the entire European Union, it would be both artificial and awkward if this meant that the same result must always be applied in every instance. This consequence arises both as a result of common sense, and EU legal principles, such as subsidiarity and proportionality. Further, these variations have been seen to play an important political and practical role.

The wisdom of these seemingly fractured approaches, built into the GDPR and highlighted by the *Google LLC v. CNIL* case, can inform the ongoing debate in the United States about how to structure privacy law in a federal system. The next Section explores how the principles of subsidiarity and proportionality that explicitly shape the EU system might caution against preemptive federal privacy law.

III. LESSONS FOR THE UNITED STATES FROM *GOOGLE LLC V. CNIL*: SUBSIDIARITY AND PROPORTIONALITY

A. The GDPR Example: Not So Monolithic and Not So Hostile to Competing Interests

The *Google LLC v. CNIL* decision reveals that the EU data protection model is less centralized and less burdensome on competing interests than commonly thought. This reality should inform the debate in the United States about broad preemptive privacy law.[137] The GDPR example and the underlying principles of subsidiarity and proportionality argue for caution regarding solutions that would limit states or impose a singular approach for balancing privacy with freedoms of speech and of the press and the related interest in access to information.

In the United States, advocates for stronger privacy throughout the country support a federal floor of protection perhaps with less sectoral variation to provide a less confusing set of expectations for individuals.[138] Privacy advocates have expressed doubt that federal efforts will produce protection that is strong enough to warrant trading away innovative law that is being passed in some states.[139] Those who seek to collect and use personal information also support federal privacy legislation but generally for different reasons. Data

---

[137] While the specific issues of territoriality of the erasure law can inform the comparatively small pockets of erasure law in the United States or even internet jurisdiction considerations more broadly, those issues are not the focus of this article. *See generally* Amy Gajda, *Privacy, Press, and the Right to Be Forgotten in the United States,* 93 WASH. L. REV. 201 (2018) (finding evidence of erasure-style protections in U.S. law and warning against expansion); David Hoffman, Paula Bruening & Sophia Carter, *The Right to Obscurity: How We Can Implement the Google Spain Decision,* 17 N.C.J.L. & TECH. 437, 474–78 (2016) (highlighting U.S. erasure law, comparing with other countries' protections, and recommending a global internet obscurity center to guide balancing of interests in internet search erasure claims); Joel R. Reidenberg, *Technology and Internet Jurisdiction,* 153 U. PA. L. REV. 1951 (2005) (arguing for preservation of rule of law by jurisdiction in the context of the internet).

[138] *California AG Opposes Federal Preemption,* EPIC.ORG (Feb. 26, 2020), https://epic.org/2020/02/california-ag-opposes-federal-.html [https://perma.cc/FK3N-Q4KY] (noting the advocacy organization's endorsement of draft legislation that would not preempt stronger state privacy laws).

[139] *See id*.

users seek legislation that would create trust and induce sharing of personal information to support its use, that would reduce what is seen as unfair inconsistencies across sectors and media, and that would simplify and reduce costs of compliance across jurisdictions. Preemption is an important goal for most data users.[140]

The GDPR is a touchstone for this debate. Although the EU form of privacy harmonization has been explained and promoted, the true extent of deference and balancing in the GDPR remains largely underappreciated in the United States.[141] In the United States, the 99 Articles and 173 preamble recitals of the GDPR have been viewed as broad and strong support for individuals' rights to data protection. The GDPR has been described as "sweeping,"[142] "strict,"[143] and as a "framework that harmonizes data protection rules across the European Union."[144] Certainly, the GDPR is broader than any one or even the sum of the sectoral sorts of federal privacy laws of the United States.[145] And, the overall impact of the GDPR is widely

---

[140] *See* CAMERON F. KERRY ET AL., BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION 16–19 (2020) (reviewing federal privacy law proposals and detailing policy recommendations including tailored preemption provisions).

[141] *See* Bilyana Petkova, *The Safeguards of Privacy Federalism,* 20 LEWIS & CLARK L. REV. 595, 632–38 (2016) (outlining the principles of subsidiarity and proportionality that govern the distribution of authority for the European Union and for Member States).

[142] Elizabeth R. Pike, *Defending Data Towards Ethical Protections and Comprehensive Data Governance*, 69 EMORY L.J. 687, 716 (2020) ("In May 2018, the European Union's sweeping data privacy law, the GDPR, came into effect."); Aarti Shahani, *3 Things You Should Know About Europe's Sweeping New Privacy Law,* NPR (May 24, 2018, 11:37 AM), https://www.npr.org/sections/alltechconsidered/2018/05/24/613983268/a-cheat-sheet-on-europe-s-sweeping-privacy-law [https://perma.cc/8KPE-YPVB].

[143] Lisa V. Zivkovic, *The Alignment Between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protect the Data Subject*, 28 TRANSNAT'L L. & CONTEMP. PROBS. 189, 210 (2018) (describing GDPR standards as strict though vague).

[144] *EU General Data Protection Regulation,* EPIC.ORG, https://www.epic.org/international/gdpr/ [https://perma.cc/XR7A-RQ92] (last visited Aug. 9, 2020).

[145] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR,* 98 DENVER L. REV. 93, 106 (2020) ("[T]he U.S. federal statutory approach is sectoral rather than omnibus (that is, comprehensive) like the GDPR–federal U.S.

viewed as providing individuals with more control over information about themselves.[146] The European Union itself has determined that the flow of personal data from the European Union to the United States must be carefully conditioned because U.S. law is deemed not "adequate" to meet strong EU standards.[147] As the United States debates new national privacy legislation, some describe the proposals as strong omnibus legislation in the style of the GDPR.[148]

As Section II of this Article showed, the *Google LLC v. CNIL* decision highlights decentralizing aspects of the GDPR. These aspects of the regulation are counter to common impressions of the EU regulation.[149] This Section examines the concepts of subsidiarity and proportionality that are evident in law that forms the backdrop for the ECJ's limitations on erasure territoriality in the *Google LLC v. CNIL* judgment. Explicit considerations of subsidiarity and proportionality do not feature prominently in the legal lexicon of the United States.[150] The EU example suggests that some attention to

---

privacy statutes do not cover all personal data, but only data in particular sectors, or held by particular entities.").

[146] Chris Jay Hoofnagle, Bart van de Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means,* 28 INFO. & COMMC'NS TECH. L. 65, 88 ("Europeans enjoy unparalleled data subject rights; they can access, rectify, and erase personal data, and have the right to object to, or restrict, processing.").

[147] The GDPR, *supra* note 2, at art. 45. Two arrangements that supported the transfer of EU persons' data to the United States have been invalidated as not sufficient for EU data protection standards. *See* Case C-362/14 Maximillian Schrems v Data Prot. Comm'r*.,* ECLI:EU:C:2015:650, *passim* (Oct. 6, 2015); Case C-311/18 Data Prot. Comm'r v Facebook Ireland Ltd., Maximilian Schrems and intervening parties, ECLI:EU:C:2019:1145, *passim* (Dec. 19, 2019).

[148] *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U.L. Rev. 771 (2019) (outlining reasons why the EU omnibus model has influenced privacy law trends around the world).

[149] *See* Oskar J. Gstrein, *Right to be Forgotten: European Data Imperialism, National Privilege, or Universal Human Right?* 13 REV. EUR. ADMIN. L. 125, 151–52 (2020) (noting "[a]t first this [case] seems surprising, . . . [h]owever . . . the substantive development of delisting has become a multi-layer and multi-stakeholder exercise with some space for diversity, also within Europe").

[150] *See* RONALD J. KROTOSZYNSKI, JR., PRIVACY REVISITED 148–250, (2016) (comparing the European and U.S. approaches to balancing competing rights, describing the process as pre-application of the right in the United States and post-application in Europe).

both principles may be useful as the United States considers new federal privacy legislation.

B. Subsidiarity as a Guiding Principle in EU Law and Evident in Google LLC v. CNIL

Subsidiarity is a principle explicitly incorporated into the law that shapes the European Union. Controlling language states that

> Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.[151]

Scholars debate subsidiarity's meaning, its purpose, factors for application, and its utility.[152] Nonetheless, this squishy principle is evident in many parts of the GDPR, including Article 17 provisions for the right to erasure, and the *Google LLC v. CNIL* decision is consistent with these limitations on centralization.

The goals of a centralized and strong data protection law are reflected in the regulation form of the law, in the language of the recitals, and in some provisions of the GDPR. Stakeholders involved in the passage of the EU law touted the new law's uniformity.[153] But,

---

[151] TEU, *supra* note 20, at art. 5(3).

[152] *See generally*, *e.g.*, David Lazer & Vikto Mayer-Schoenberger, *Blueprints for Change: Devolution and Subsidiarity in the United States and the European Union, in* FEDERAL VISION: LEGITIMACY AND LEVELS OF GOVERNANCE IN THE UNITED STATES AND THE EUROPEAN UNION, 118–43 (Kalypso Nicolaidis and Robert Howse eds., 2003) (ebook) (reviewing policy and law in the EU and the United States addressing proper allocation of authority between central governing bodies and component states, and finding as of 2001, more procedural criteria than substantive restrictions on central authority); Paolo G. Carozza, *Subsidiarity as a Structural Principle of International Human Rights Law*, 97 AM. J. INT'L L. 38 (2003) (exploring the history and purpose of subsidiarity); Andreas Føllesdal, *Competing Conceptions of Subsidiarity* in. NOMOS LV: FEDERALISM AND SUBSIDIARITY (2014) (assessing the effectiveness of different implementations of subsidiarity); Andreas Follesdal, *Competing Conceptions of Subsidiarity* (2013) (Univ. of Oslo Fac. of L., PluriCourts Rsch. Paper No. 2013-35) https://ssrn.com/abstract=2359964 [https://perma.cc/S6CK-DA6Y] ("[C]onsiderations of subsidiarity will seldom resolve disagreements about the allocation of authority.").

[153] Vivian Reading, *Foreword* to MONIKA KUSCHEWSKY, DATA PROTECTION & PRIVACY: JURISDICTIONAL COMPARISONS, at viii (2012) (writing as Vice-

several components of the law including the Recitals, Provisions for harmonization of Member States' implementations, Article 85, and the erasure provision itself include nontrivial acknowledgement of the retention of Member States' own authority to enact and apply the law in potentially varying ways. The ECJ considered some of these dueling forces in its opinion limiting the automatic pan-EU application of search engine erasure actions.

Perhaps tellingly, the ECJ did not identify the regulation form of the GDPR as a factor in its analysis of whether EU law required a pan-EU territorial scope for erasure in search engine de-listing cases. Generally, the regulation form of the EU law gives more authority to the European Union than a directive.[154] Regulations constitute directly applicable law, while directives provide a framework that Member States are expected to use as guides for enacting national implementing law.[155] Statements of officials[156] and

---

President and Member of the European Commission responsible for Justice, Fundamental Rights, and Citizenship: "[g]lobalization, economic integration and technical progress are international processes by default. As a result, businesses my increasingly find themselves in violation of laws in some countries . . . .data protection reform . . . will simplify and harmonise legal requirements in the EU, and provide a level playing field for businesses.").

[154] VAN DER SLOOT, *supra* note 12, at 17. *But see* Julian Wagner & Alexander Benecke, *National Legislation with the Framework of the GDPR,* 2 EUR. DATA PROT. L. REV. 353, 359–60 (2016) (exploring the potential for and legality of complexity due to national laws permitted under the GDPR); Simon Davies, *The Data Protection Regulation: A Triumph of Pragmatism over Principle?* 2 EUR. DATA PROT. L. REV. 290, 294–95 (2016) ("The Regulation was originally intended to obviate the need for implementing legislation at the national level, and would thus create a harmonized framework.").

[155] TFEU, *supra* note 19, at art. 288.

[156] Giovanni Buttarelli, European Data Protection Supervisor, praised the Regulation and noted it centralizes accountability and "promises a wider scope for cooperation . . . both within the EU and internationally." *The EU GDPR as a Clarion Call for a New Global Digital Gold Standard*, 6 INT'L. DATA PRIV. L. 77 (2016) (noting the Regulation); Duncan Robinson, *Companies Attach Imbalance in Data Protection Rules,* FIN. TIMES (DEC. 16, 2015), https://www.ft.com/content/781c9bc4-a402-11e5-873f-68411a84f346 [https://perma.cc/GB5S-SNEU] (quoting Jan Philipp Albrecht, Member of the European Parliament who helped draft the GDPR: "[t]he new rules will give businesses legal certainty by creating one common data protection standard across Europe.").

analysis by stakeholders[157] throughout the legislative process promoted the uniformity that would be achieved with the new type of law. One reason the ECJ neglected this point may be that the Court was looking to both the prior law, the DPD, and to the newer GDPR due to the progress of the case spanning the replacement of the Directive with the Regulation.[158] But, as was explored in Section II above, another reason that the ECJ may have neglected the central authority of the Regulation is that the GDPR contains many relevant preamble sections as well as provisions that enable and even require a more decentralized approach to balancing data protection with competing interests such as expression and access to information, especially in the context of erasure rights and exceptions to erasure rights.

The *Google LLC v. CNIL* decision identifies as relevant to its deliberations several GDPR recitals that articulate goals for uniformity of data protection throughout the European Union and explain the purposes of uniformity.[159] The ECJ noted Recital 9, which states that the Directive's objectives and principles:

---

[157] Arthur Piper, *Data Protection Across the Pond: The Implications of the EU's New Data Privacy Law*, 63 RISK MANAGEMENT 32, 34 (Jan. 1, 2016) ("Even if businesses don't relish the prospect of stricter requirements, there are still things to like about the incoming regime. For one thing, Europe will have a unified set of rules governing the use of data that applies in exactly the same way in each of its member countries."); Robinson, *supra* note 156 (quoting a spokesperson for Facebook: "Having a single set of rules to protect Europeans' personal data while creating opportunities for growth and innovation is important for people in Europe and the European economy"). *But see Data Protection Agreement to Bring Major Changes to EU Privacy Law*, CTR. FOR DEMOCRACY & TECH. (Dec. 15, 2015), https://cdt.org/press/data-protection-agreement-to-bring-major-changes-to-eu-privacy-law/ [https://perma.cc/WWU9-ZGYL] ("The goal of the data regulation reform was to replace the existing patchwork of national laws with one common regulation . . . An important question is whether this Regulation will be implemented in a uniform way across the EU.").

[158] Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶ 41 (Sept. 24, 2019) (judgment).

[159] It is worth emphasizing at this stage that recitals form part of the preamble for EU legislation and so are not legally binding, rather acting as interpretive guidelines for the actual Articles which make up the binding law. European Union, Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation (2015), Guidelines 7 and 10, at 24, 31–36.

> [R]emain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity.[160]

The different levels of protection in Member States are said to impede the free flow of information throughout the European Union and "constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law."[161] These preamble statements support the popular notion of the EU law as omnibus and uniform.

The ECJ also refers to the consistency and high level of data protection goals articulated in Recital 10 before reaching a conclusion that interests in competing rights may vary from one Member State to another.[162] Recital 10 reflects the consistency goals of the GDPR but also the difficulties of fully achieving consistency.[163] Recital 10 states:

> In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.[164]

Nonetheless, Recital 10 continues by outlining ways that Member States "should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation."[165] Processing for compliance with a legal obligation, presumably including under Member State law, is noted as an area

---

[160] The GDPR, *supra* note 2, at Recital 9; *Google LLC v. CNIL* (judgment), ¶ 13.

[161] The GDPR, *supra* note 2, at Recital 9.

[162] *Google LLC v. CNIL* (judgment), ¶ 67.

[163] The GDPR, *supra* note 2, at Recitals 10 and 13. *See also* The GDPR, *supra* note 2, at 119, 129 ("In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union.").

[164] *Id.* at Recital 10.

[165] *Id*.

where Member States maintain authority.[166] Processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller are also noted as areas for national authority.[167] Member States are further given "a margin of manoeuvre" to specify their own rules including those applying to data categorized as sensitive.[168] The recital concludes with "[t]o that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful."[169] These carve-outs allow for significant Member State variations in the shape of data protection law.

The ECJ also notes several articles of the text of the GDPR that outline processes for Member States' Data Protection Authorities to cooperate, provide mutual assistance, and conduct joint operations.[170] While the DPD contained some provisions which required collaboration and cooperation between national Data Protection Authorities,[171] consistency in implementation and enforcement was nonetheless widely criticized.[172] So, provisions in

---

[166] *See, e.g.*, Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 19.

[167] *Id.*

[168] *Id.*

[169] The GDPR, *supra* note 2, at Recital 10. Other Recitals note areas in which the EU Regulation would not apply due to broader limits on the scope of EU law in the context of national security or the separate authority of other EU law to address crime or the deference to Member States for addressing processing of data of deceased persons. The GDPR, *supra* note 2, at Recitals 16, 19, 27.

[170] Case C-507/17 Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 ¶¶ 68–69 (Sept. 24, 2019) (judgment) (referring to articles 56, 60, 61, 63–66).

[171] The DPD, *supra* note 29, at art. 28(6).

[172] *See generally* Douwe Korff, EC Study on Implementation of Data Protection Directive, Annex 3 (2002) (conducting an extensive comparative study of national laws implementing the Data Protection Direction and noting throughout variations in Member States' approaches); Douwe Korff, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments* (Eur. Comm'n, Working Paper No. 2, 2010) (highlighting different approaches to evolving privacy risks within the European Union and noting significant non-harmonization). It is also worth noting that the

the newer GDPR provide more formal requirements outlining scope of authority for individual Member States' data protection supervisory authorities as well as robust procedures to support requirements reconciling the variations.[173] Interestingly, though, as explained in Section II, the ECJ found these provisions for consistency did not provide a general cue that erasure for internet personal name searches should as a rule result in exactly the same result simply being copy-pasted throughout the European Union.[174] Instead, the Court concluded that these GDPR procedural harmonization provisions provide an avenue for consideration of how erasure rights of a resident of one nation might be balanced differently or even consistently throughout the European Union.[175]

The reality is that the GDPR text itself seems to retain elements of a directive with specific delegations of responsibilities to Member States to enact enabling laws.[176] The Article 17 right to erasure's exception for balancing data protection with competing rights of expression and information exist alongside Article 85, which reflects significant reliance on Member States in requiring each to enact laws to balance these freedoms and provide regular reports to the European Union on how these national laws achieve a proper balancing. Other delegations of responsibilities to Member States appear in the GDPR, some allowing for "more specific provisions"

European Commission noted that this issue still remains to some extent under the GDPR and that they consider this to be a goal for the ongoing implementation of the GDPR. European Commission, Communication from the Commission to the European Parliament and the Council: Data Protection as a pillar of citizens' empowerment and the European Union's approach to the digital transition – two years of application of the General Data Protection Regulation {SWD(2020) 115 final}, COM(2020) 264 final, 5–6.

[173] *Google LLC v. CNIL* (judgment), ¶ 68.

[174] *See supra* Section II.

[175] *Google LLC v. CNIL* (judgment), ¶ 69.

[176] Simon Davies, *The Data Protection Regulation: A Triumph of Pragmatism over Principle*, 2 EUR. DAT. PROT. L. REV. 290, 294–95 (2016) ("The Regulation was originally intended to obviate the need for implementing legislation at the national level, and would thus create a harmonised framework. This aim has failed substantially.").

and some allowances when they are "necessary and proportionate."[177]

In general, the GDPR reveals substantial elements of subsidiarity in the authority afforded to, or competency retained by, Member States. These responsibilities allow for differentiation, but it remains to be seen just how EU Member States will distinguish themselves or follow similar paths in enacting national legislation under Article 85 or in interpreting such provisions as Article 17's right to erasure. After more time with the GDPR in place, analysis of the efficacy of these harmonization processes may tell more about how much harmonization this procedural framework produces. Similarly, comparisons of Article 85 reports and legislation may provide interesting insights into the level of variation across the European Union in balancing data protection with expression and information.

Subsidiarity in the United States is arguably integral to the formal allocations of authority of the federal government and the states both in the Constitution and in federal courts' interpretations of those Constitutional provisions.[178] Even if U.S. Constitutional constraints on federal authority do not prevent preemptive and broad federal privacy law, subsidiarity should inform the political debate

---

[177] Article 6(2) and Article 6(3) allow Member States to provide greater clarity to what is meant by lawfulness of processing. The GDPR, *supra* note 2, at arts. 6(2), 6(3), 23. Article 23 provides room for Member State legislation to restrict the scope of several articulated obligations and rights under the GDPR "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard . . . ." *Id.*

[178] *See* Alex Mills, *Federalism in the European Union and the United States: Subsidiarity, Private Law, and the Conflict of Laws,* 32 U. PA. J. INT'L L. 369, 371 (2010) (comparing subsidiarity in the United States and the European Union and asserting the principle has a "largely latent but potentially important role in the United States."); Steven G. Calabresi & Lucy D. Bickford, *Federalism and Subsidiarity: Perspectives from U.S. Constitutional Law,* in FEDERALISM & SUBSIDIARITY: NOMOS LV 123 (J. E. Fleming & J. T. Levy eds., 2014) (exploring subsidiarity in the context of U.S. constitutional federalism and arguing that U.S. subsidiarity should be enforce through judicial review).

about the appropriateness of a truly omnibus and preemptive federal law.[179]

The EU model suggests that creation of a new preemptive U.S. federal law might not be better just because the law itself purports to offer uniform protections to individuals and to simplify compliance. The impact of a broadly applicable law could be unequal based on the factual and cultural differences that shape life in different parts of the United States.[180] Shared experiences of history and culture can produce differing levels of commitment to access to information and to the expressive rights of sharing information, particularly in comparison with commitment to privacy or data protection.[181] And some data users, like Google and amicus companies, like Microsoft who supported the Google position, might argue against the simplicity of a uniform compliance approach, if they are able to advance their business goals more in some jurisdictions than they would under a single federal law.[182]

---

[179] Mills, *supra* note 178, at 431 (noting that subsidiarity is viewed as "playing only a very limited role in the U.S. federal system, and then only as a political rather than a legal principle").

[180] Beate Rössler in her book, THE VALUE OF PRIVACY 13 (2005), notes that there is very little treatment of cultural variations in privacy among Western democracies, though anthropology and ethnology studies compare Western and non-Western privacy cultures. *See* Alison Cool, *Impossible, Unknowable, Accountable: Dramas and dilemmas of data law,* 49 SOC. STUD. SCI. 503, 504 (2019) ("The Second World War has cast a long shadow on data practices in Europe. In France and Germany in particular, centralized national data collection and interlinkage through personal identification numbers are still viewed as problematic and suspicious . . . . In the Nordic countries, however, a strong historical relationship between the social welfare state, national population registries and data-driven policy has provided another lens through which extensive and centralized data collection appears if not beneficial, then at least not inherently negative.").

[181] *See*, *e.g.*, Sharon K. Sandeen & Ulla-Maija Mylly, *Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing*, 21 N.C. J.L. & TECH. 1 (2020).

[182] Jean Gonié, *Foreword* to MONIKA KUSCHEWSKY, DATA PROTECTION & PRIVACY: JURISDICTIONAL COMPARISONS at xiii (2012) (writing as Director of Privacy, EU Affairs, for Microsoft: "[t]rying to understand the way the current patchwork of national and regional law around the world applies is, of course, a priority for the legal ecosystem. But not every size of company can do so easily because they lack resources.").

C. Proportionality, Working in Concert with Subsidiarity in Google LLC v. CNIL

Like subsidiarity, proportionality is a foundational concept in documents that shape the European Union.[183] Protocol (No. 2) of the Treaty on the Functioning of the European Union ("TEU") requires that any draft legislation "should contain a detailed statement making it possible to appraise compliance with the principles of subsidiarity and proportionality."[184] Draft acts are required to minimize the burden of the legislation on organizations and individuals and be "commensurate with the objective to be achieved."[185] Proportionality can be thought of as limiting legal solutions to those that match in some way the value of its impact. The concept is one that connotes restraint so that legal solutions are not overly restrictive. The principle has deep roots in European law and has inspired sophisticated assessments of the proper meaning and application.[186] The concept is often associated with balancing competing rights or interests,[187] and judicial review.[188]

---

[183] TEU, *supra* note 20, at art. 5. *See also* 2012 O.J. (C 326) 1, 207, https://eur-lex.europa.eu/resource.html?uri=cellar:c382f65d-618a-4c72-9135-1e68087499fa.0006.02/DOC_4&format=PDF [https://perma.cc/7R4D-ZWJE] on the application of the principles of subsidiarity and proportionality (outlining the need for a means for securing respect both principles).

[184] 2012 O.J. (C 326), at 207.

[185] TEU, *supra* note 20, at art. 5.

[186] Eric Engle, *The History of the General Principle of Proportionality*, 10 Dartmouth L.J. 1 (2012) (examining the history of the principle of proportionality from Aristotle to contemporary law); Audrey Guinchard, *Taking Proportionality Seriously: The Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law,* 24 EUR. L.J. 434(2018) (building on the framework of contextual integrity to create a systematic method of evaluating and implementing proportionality in EU data protection law).

[187] AHARON BARAK, PROPORTIONALITY: CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS 235 (2012) (examining the necessity and utility of proportionality).

[188] Alec Stone Sweet & Jud Mathews, *Proportionality Balancing and Global Constitutionalism,* 47 COLUM. J. TRANSNAT'L L. 72, 86–88 (2008-09) (describing how courts avoid declaring one right as absolute in contrast with competing rights by moving into balancing interests through the lens of proportionality); Vikki C. Jackson, *Constitutional Law in an Age of Proportionality,* 124 YALE L.J. 3094, 3136–53 (2015) (arguing for a moderate increase in proportionality analysis in U.S. Constitutional review and exploring specifically how it might serve in First Amendment cases).

Recital 4 of the GDPR addresses proportionality in describing data protection as a qualified right. The protection of personal data "is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[189] In fact, Recital 4 highlights the need to also protect several other rights that tend to compete with data protection, including freedom of expression and information as well as freedom to conduct a business.[190]

Because data protection and privacy are commonly in conflict with expression and information access, proportionality is an important and perhaps intuitively useful tool for evaluating whether a balance is appropriate. The ECJ decision reflects attention to proportionality in declining to require broad territoriality in the particular context of erasure claims at issues in *Google LLC v. CNIL*.

Much of the subsidiarity described in the prior Section addresses EU Member States' requirements to conduct proportionality tests in applying Article 17 erasure rights to particular cases and in passing laws under Article 85 to address national standards for balancing data protection with expression and information rights. The two principles may be intertwined in many contexts but certainly are in conversation in data protection in recognition of national variation in cultural norms and in particular case impacts. Because of these principles and norms, the GDPR actually contains support for tipping the scales away from data protection when needed to protect expression and information. The *Google LLC v. CNIL* decision highlights this restraint in data protection.

In the United States, these EU accommodations of expression and information in the context of the GDPR may be underappreciated. In general, the impression in the United States is that the GDPR created data protection that overly burdens rights of expression and information that are similar to First Amendment

---

[189] The GDPR, *supra* note 2, at Recital 4.

[190] The European Charter of Fundamental Rights includes the freedom to conduct a business as one of the protected liberties in the same section of the Charter as data protection. The Charter, *supra* note 14, at art. 16.

freedoms of speech and of the press.[191] The ECJ acknowledged in the *Google LLC v. CNIL* decision that countries around the world may place different emphases on the relative weight of the freedom of expression.[192] But this acknowledged comparative difference in the value placed on expression may create an exaggerated conception of the EU's preference for data protection. The *Google LLC v. CNIL* decision and the text of the GDPR itself provide evidence that expression and information rights are still valued under the EU model for data protection. Even in this strong and detailed data protection regulation, significant accommodation remains for these competing interests.

In the United States, the protections for speech and for the press are similar to the rights of expression and information in the European Union. Judicial review of burdens on these Constitutional rights in the United States is complex and arguably hides proportionality analysis that is actually being employed.[193] The tide may be turning towards scholarly acceptance of proportionality analysis in U.S. Constitutional law.[194] However, in the context of data protection or privacy law, objections to proportionality assessments on a case-by-case basis are likely to target a lack of predictability for both rights holders and information users. Predictability and risk management are a significant part of the

---

[191] Mike Masnick, *Dear Europe: Please Don't Kill Free Speech in the Name of 'Privacy Protection',* TECHDIRT (May 8, 2017) (arguing that the EU right to be forgotten could lead to over-restriction of speech). *See* Amy Gajda, *Privacy, Press, and the Right to be Forgotten in the United States,* 93 WASH. L. REV. 201, 264 (2018) (highlighting examples of erasure-like protections in U.S. law and warning that the United States must determine how to "cabin a Right to Be Forgotten effectively with a way that strongly and nearly always support press freedoms").

[192] Case C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶ 60 (Sept. 24, 2019) (judgment).

[193] *See* Jackson, *supra* note 188; Evelyn Douek, *Governing Online Speech: From "Posts-as-Trumps" to Proportionality & Probability,* 121 COLUM. L. REV. (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3679607 [https://perma.cc/Y2WW-4B6H].

[194] *See* Jackson, *supra* note 186.

debate in the United States regarding new federal privacy legislation.[195]

Whether or not proportionality is itself transferable to the United States, the lesson from *Google LLC v. CNIL* may be to recognize the EU data protection model is not a set of requirements that inflexibly favors data protection over competing rights. The GDPR actually provides protections that are strong but qualified, with some balancing incorporated and some deferred. The result is a law that can accommodate evolving data uses and norms. As the United States struggles to find the appropriate and predictable balance for potential federal privacy legislation, the EU example can serve as fair warning that some questions will require ongoing consideration through either courts or other processes such as regulatory action.

IV. CONCLUSION

Google LLC v. CNIL delivered a somewhat surprising modesty of territorial scope for the erasure rights at issue in internet personal name searches. The ECJ judgment surfaces the GDPR's features of decentralization and ongoing balancing of the qualified right of data protection with expression and information rights. While the Court left a number of questions unanswered in its reasoning, subsidiarity and proportionality are evident in the decision.

As the United States considers the GDPR as a touchstone for broad new federal legislation, these two moderating concepts should reshape the U.S. understanding of the influential EU example. This EU regulation is not the uniform static set of protections that some assume. The United States should also take a measured approach to both preemption and to the feasibility of thoroughly anticipating how to balance privacy with competing interests. The United States

---

[195] Cameron F. Kerry et al., *Bridging the gaps: A path forward to federal privacy legislation*, BROOKINGS (June 3, 2020) (noting "the single most important reason for industry to accept and support federal privacy legislation is an understandable desire for a single national set of rules to follow."); David Hoffman, Paula Bruening & Sophia Carter, *The Right to Obscurity: How We Can Implement the Google Spain Decision*, 17 N.C. J.L. & TECH. 437, 477–80 (2016) (advocating for the creation of a Global Internet Obscurity Center to guide search engines challenged by the need to balance expression and information rights with requests under the EU right to be forgotten).

should note that the EU legislative process took four years and has been described as "tortuous." Deciding on the best allocation of authority and on the level of information privacy or data protection is likely to be no easier in the United States than in the European Union.[196]

[196] Simon Davies, *The Data Protection Regulation: A Triumph of Pragmatism over Principle?*, 2 EUR. DATA PROT. L. REV. 290, 290 (2016) (describing the four years of passage of the GDPR as "tortuous," "accompanied by aggressive lobbying by corporate interests and by a sometimes intransigent EU Council").