The Right to Erasure: Evaluating the U.K. Approach to GDPR Article 17

Editors: Grant Fergusson, Kristen Shiu

Writers: Matt Ireland, Stephanie Metzger, Ugonma Nwankwo,
Stefan Tan Ying Xian, Grant Fergusson, Kristen Shiu

The Wilberforce Society
Cambridge, UK

www.thewilberforcesociety.co.uk
October 2019

ACKNOWLEDGEMENTS

Special thanks to Haley Rice and Bryan Fong for their organizational support and to Dr. Jennifer Cobbe and Dr. Tanya Filer for their advice and feedback.

ABSTRACT

The General Data Protection Regulation (GDPR) is the most comprehensive set of data protection regulations ever implemented. Nevertheless, its attempt to address unique challenges to data protection today, while both positive and progressive, has raised many questions for policymakers and organizations as they seek to comply with it. In particular, GDPR Article 17, which formalises a right to erasure (commonly referred to as 'the right to be forgotten'), has faced numerous criticisms and implementational challenges.

This paper aims to provide a deeper analysis of the development, implementation, compliance, and enforcement of GDPR Article 17 within the U.K. context to highlight key political and technological challenges that GDPR must overcome. This paper then proposes a variety of recommendations aimed to improve the overall effectiveness of GDPR within the U.K. given the nation's current political and technological characteristics.

EXECUTIVE SUMMARY

Overview

Since the first public demonstration in 1972 of the Advanced Research Projects Agency Network (ARPANET)—the first iteration of what would later become the internet—global internet access has increased at breakneck speed and the world's data environment has changed substantially[1]. With the rise of internet access came myriad new and rapidly growing industries—from telecommunications to software development—that today account for 4% of the United Kingdom's employment and 7% of its economic output[2]. Moreover, digital industries are growing at more than double the rate of the U.K.'s overall gross domestic product[3].

As digital companies and governments alike have turned to data analytics to improve the effectiveness and commercial viability[4] of digital products and services amid these rapid changes, policymakers in the U.K. and abroad have developed various regulations designed to protect the rights of citizens and their data online. The European Union's General Data Protection Regulation (GDPR), enacted in 2016 and implemented in 2018, is the most recent and perhaps the most comprehensive of these policies, establishing robust enforcement and accountability procedures, strengthening existing data policies, and enshrining several digital rights into law for the first time. Despite these advances, GDPR critics have raised several concerns regarding its implementation. In particular, GDPR Article 17—which formalizes a right to erasure (commonly referred to as 'the right to be forgotten')—has faced several legal battles from both digital firms seeking to reduce their compliance requirements and data protection advocates who believe the regulation's principles-based enforcement mechanisms fail to adequately protect citizens[5]. As the

[1] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, & Stephen Wolff, 'A brief history of the Internet', *ACM SIGCOMM Computer Communication Review*, 39/5, 22-31 (2009).
[2] Chris Rhodes & Georgina Hutton, 'The Future of the U.K. digital and tech industries'. [Debate Pack], (2018), House of Commons Library, CDP 2018/0096, <http://researchbriefings.files.parliament.uk/documents/CDP-2018-0096/CDP-2018-0096.pdf>.
[3] Umar Hassan, 'U.K. Tech Sector Booms to £184 Billion as "Digital Suburbs" Emerge'. [Website], (2018), Computer Business Review. <https://www.cbronline.com/news/uk-tech-sector-growing-2-6-times-faster-national-gdp>.
[4] See Shoshana Zuboff, 'Big other: Surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology,* 30/1, 75-89 (2015).
[5] Josephine Woolf, 'How Is the GDPR Doing?'. [Website], (2019), Slate. <https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html>

U.K. attempts to simultaneously protect its citizens' data and foster greater digital innovation[6], U.K. policymakers will need to carefully consider how their approach to GDPR has fared in the year since it was first enforced. GDPR Article 17, which has faced considerable legal, regulatory, and compliance hurdles since it was first implemented, is well-positioned to provide U.K. policymakers with valuable insight into the U.K.'s approach to data protections and digital innovation overall.

Purpose of this Report

U.K. citizens increasingly do business with companies around the world and rely on digital technologies at home and abroad, making the U.K. digital economy both an invaluable tool to boost the U.K.'s overall economy and a potential risk factor for U.K. data security[7]. While the U.K. government has developed a variety of data policy approaches to foster the U.K.'s growing digital sector and protect citizens' data rights, it has only recently begun to focus more on the effectiveness of its approach[8]. Given the speed of technological advancement and the growing centrality of citizen data to the digital sector[9], the U.K. government will need to regularly assess and update its approaches to data policy. This report serves as a preliminary evaluation of one such data policy—GDPR Article 17—that has faced particularly extreme legal and regulatory challenges in the year since GDPR was first enforced. By considering both Article 17 and its relevant U.K. regulatory procedures within their historical and geopolitical context, this report attempts to highlight the strengths and weaknesses of the U.K.'s current policy approach and suggests ways to improve enforcement and compliance procedures as U.K. policymakers re-evaluate and advance their national data strategy.

[6] Information Commissioner's Office, 'Information Commissioner's Office Innovation Plan – April 2017'. [Website], (2017), ICO. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/608843/ICO_Innovation_Plan_April_2017__1_.pdf>.
[7] U.K. Department for Digital, Culture, Media & Sport, 'Cyber Security Breaches Survey 2019', [Website], 2019, GOV.UK. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf>
[8] Information Commissioner's Office, 'Information Rights Strategic Plan 2017-2021' [Website], 2017, ICO. <https://ico.org.uk/media/about-the-ico/documents/2014134/20170413icoinformationrightsstrategicplan2017to2021v10.pdf>
[9] European Commission, 'Big data and digital platforms' [Website], European Commission. <https://ec.europa.eu/growth/industry/policy/digital-transformation/big-data-digital-platforms_en>

In evaluating policies regarding the right to erasure, this report considers not only direct implementational and enforcement challenges, but also the various commercial and geopolitical implications that policies surrounding the right to erasure may have. In doing so, this report aims to provide U.K. policymakers with the tools and knowledge they need to develop comprehensive and responsive policies surrounding the right to erasure both now and in a post-Brexit world.

Recommendations

Given the challenges of interpreting and enforcing GDPR and Article 17, this paper also provides some recommendations aimed at making organizations, the U.K. civil service, and individuals more capable of handling them. In particular, the U.K.'s Information Commissioner's Office (ICO) can help organizations through increasing supporting services that would help them address and invest more in GDPR compliance. At the same time, the institutional capacity of the civil service should also be strengthened to provide effective regulatory oversight. Finally, raising awareness around data protection issues at the individual level and making people more cognizant of their rights under GDPR is a critical step in making GDPR more effective.

Limitations

Although this report aims to be as thorough as possible in considering the right to erasure and the impact of Brexit, the current political and policy environments in the U.K. and the general uncertainty surrounding GDPR due to its recent implementation mean that the practical specifications and future applications of GDPR are subject to change. Additionally, ensuring total compliance with GDPR through comprehensive oversight efforts is difficult because it would require significant resources and an intimate understanding of the inner workings of many organizations; consequently, compliance duties are dispersed between the European Data Protection Board, E.U. member states' data protection authorities, these private organizations, and the court system, many of whom have different priorities and interpretations of GDPR. Nevertheless, by contextualizing the right to erasure in recent history and providing recommendations aimed at strengthening enforcement and compliance, this report addresses the benefits and challenges of a critical provision within GDPR. Furthermore, while these recommendations are broad and would require additional resources from DCMS and the ICO, they will ultimately help the U.K. in developing its legal understanding of GDPR to help

organizations comply and enable both the U.K. government and U.K. citizens to face the challenges of data protection in a progressively complex digital age.

TABLE OF CONTENTS

I. INTRODUCTION

In the year since GDPR first went into effect, U.K. companies have adopted numerous (and sometimes costly[10]) data practices to comply with new regulatory requirements[11]. For example, 92% of U.K. companies have hired Data Protection Officers (DPOs)[12], and many companies have developed or purchased new software tools to facilitate compliance procedures[13]. Despite these efforts, many companies still fail to fulfil GDPR regulatory requests within the required timeframe[14].

Most companies have focused their efforts on ensuring their existing data collection and processing practices abide by GDPR requirements[15]. However, early evidence suggests that another compliance requirement—processing right to erasure requests under GDPR Article 17—represents a large and growing portion of GDPR regulatory requests[16]. To date, there exists little published regulatory enforcement surrounding GDPR Article 17 and little evidence to suggest how effective GDPR Article 17 has been in protecting user data.

By assessing the success of GDPR Article 17 and its implementation within the U.K. in light of historical, geopolitical, and theoretical trends, this report aims to facilitate much-needed evaluations of GDPR Article 17 and assist policymakers in determining how best to approach GDPR regulation and enforcement in the future.

[10] Jeremy Kahn, Stephanie Bodoni, & Stefan Nicola, 'It'll cost billions for companies to comply with Europe's new data law'. [Website], (22 March 2018), Bloomberg Businessweek, <https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law>.
[11] Peter Gooch, Beth Dewitt, Erik Luysterbourg, Manish Sehgal, Annika Sponselee, David Batch, & Daniel P. Frank, 'A new era for privacy: GDPR six months on.' [Website], (2018), Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf>.
[12] *Ibid.*
[13] See Capterra, 'GDPR Compliance Software'. [Website], (2019). <https://www.capterra.com/gdpr-compliance-software/>.
[14] Talend, 'The majority of businesses surveyed are failing to comply with GDPR, according to new Talend research'. [Press Release], (2018), Talend. <https://www.talend.com/about-us/press-releases/the-majority-of-businesses-are-failing-to-comply-with-gdpr-according-to-new-talend-research/>.
[15] GDPR Report, 'GDPR: Getting to grips with the "right to erasure" requirement'. [Website], (2018), PrivSec Report. <https://gdpr.report/news/2018/07/11/gdpr-getting-to-grips-with-the-right-to-erasure-requirement/>.
[16] Gooch et al. (n 5).

I.I. FOUNDATIONS OF EUROPEAN DATA PROTECTION RIGHTS

i. Conceptual Foundation

Since the development of ARPANET, global internet access has increased exponentially[17]; as of 2016, almost 339 million people—roughly 45.79% of the world's population—had internet access[18]. With the growth of internet access came a slew of new legal and ethical challenges: How could laws be enforced in anonymous digital spaces? Who has jurisdiction over digital spaces? Who owns the data being sent, shared, and created in digital spaces? As the internet shifted from academic oddity to commercial success in the early 1990s[19], regulators in both Europe and the United States were forced to consider how traditional jurisprudence and ethical standards might apply to the internet[20]. They were, in short, forced to consider what rights and restrictions extended into the digital world.

American and European policymakers differed in both their conceptions of and trajectories on digital rights. While U.S. policymakers grounded their policies in long-held conceptions of privacy and autonomy[21], European policymakers tended to conceive of digital rights as data protection rights distinct from existing rights to property or privacy earlier on.[22] Still, the American and European conceptions of digital rights are based on similar ideals and are therefore intimately related. In his 2010 essay entitled 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights', Norberto Nuno Gomes de Andrade explains:

> 'The emergence of the first data protection legislations in the early 1970s, as well as their subsequent developments, were and have been aimed at tackling problems generated by new technologies. Within the broad spectrum of problems to be resolved, the application of those data protection regulatory schemes was—to a great extent—motivated by privacy concerns. In fact, one can

[17] Leiner et al. (n 1).
[18] World Bank, 'Individuals using the Internet (% of population)'. [Website], (2017), The World Bank Group. <https://data.worldbank.org/indicator/IT.NET.USER.ZS>.
[19] Encyclopaedia Britannica. 'Internet'. [Website]. Encyclopaedia Britannica. <https://www.britannica.com/technology/Internet>
[20] Leiner et al. (n 1).
[21] See Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harv. Ll. Rev. 5, 193.
[22] Molly Guinness, 'France maintains long tradition of data protection'. [Webiste], (26 January 2011), Deutsche Welle. <https://www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711>.

> say that the incessant development and sophistication of data protection legal frameworks across the last decades has taken place as a result of the fact that individuals' privacy is continuously under threat via increasingly novel means'[23].

ii. Historical Foundation

Many European nations began to develop their own data protection policies in the 1970s and 1980s. France, for example, enacted its Data Protection Act in 1978, which both guaranteed that individuals provide informed consent for data collection and processing and applied to both private and public entities that wish to collect personal data[24]. Similarly, Germany passed its Federal Data Protection Law in 1977[25], which regulated the collection and use of personal data by state and non-state actors to 'protect the individual against violations of his personal right (Personlichkeitsrecht)'[26]. Such individual rights-based policies informed the creation of broader European policies on data protection that preceded GDPR.

In 1981, the first of these Europe-wide data policies, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[27], was adopted by the Council of Europe. In addition to regulating the collection and use of personal data and data flows, the Convention 'outlaw[ed] the processing of 'sensitive' data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards' and 'enshrine[d] the individual's right to know that information is stored on him or her and, if necessary, to have it corrected'[28]. Despite the collective nature of the Convention, however, the data protection policies of European nations continued to develop independently until 1992, when the European Union was established under the Maastricht Treaty[29]. Now unified, policymakers within E.U. member states made significant efforts to consolidate and coordinate

[23] Norberto Nuno Gomes de Andrade, 'Data protection, privacy and identity: Distinguishing concepts and articulating rights' in *Privacy and Identity Management for Life* (Springer 2010).
[24] Loi N° 78-17 du 6 Janvier 1978.
[25] Gesetz zum Schutz vor MiBbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) of 27 January 1977.
[26] David Banisar & Simon Davies, 'Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments', *J Marshall J. Computer & Info. L.,* 18, 1 (1999).
[27] Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', Strasbourg, France (1981) ETS No. 108.
[28] *Ibid.*
[29] Consolidated Version of the Treaty on European Union [1992] OJ C325/5.

the data protection policies of each country. The result was the Data Protection Directive of 1995[30], which provided guidance to countries on the minimum required standards for data protection laws and outlined common practices for sharing data between member states[31]. While this directive standardized the level of data protection within the E.U., it focused more on the procedural obligations of data controllers than on the rights of individuals, stopping short of enshrining data protection rights as human rights[32]. As a result, the Data Protection Directive quickly became inadequate. De Andrade suggests why:

> 'The data protection directive is based upon the concept of privacy and constructed under a logic of identification. As such, the directive is only applicable if it processes data that allows for a specific person to be identified. In so doing, the [data protection directive] neglects the concept of identity and the logic of representation. According to the latter, what is becoming increasingly important is how data and information are being used to represent someone, and not to merely identify him or her. In other words, the issues raised by the processing of personal information cannot only be about disclosing information involving someone's privacy, but also of using such information to construct and represent someone else's identity'[33].

De Andrade's broader definition of data protection obligations highlighted the shortcomings of a process-based approach to data protection: without a rights-based approach to data protection, individuals' data could be used in harmful ways when aggregated.

Subsequent developments in European human rights law have broadly incorporated De Andrade's perspective. Article 8 of the Charter of Fundamental Rights of the European Union, originally ratified in 2000, provided E.U. citizens with broad data protection rights: 'everyone has the right to the protection of personal data concerning him or her'[34]. Importantly, it existed

[30] Council Directive (EC) 95/46 with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995].
[31] See Daniel J. Solove, 'A brief history of information privacy law' in *Proskauer on Privacy* (PLI 2006).
[32] Yvonne McDermott, 'Conceptualising the right to data protection in an era of Big Data', *Big Data & Scoiety,* 4/1, 1-7 (2017).
[33] De Andrade (n 17).
[34] 'Article 8: protection of personal data' in Charter of Fundament Rights of the European Union [2012] OJ C326/02.

independent from Article 7, which concerned the individual's right to privacy, marking the first time that data protection *rights*—as opposed to process obligations—were explicitly enumerated within law across Europe. (Notably, the right to erasure was not included in the Charter.) The shift toward a human rights approach to data protection under the Charter of Fundamental Rights of the European Union paved the way for broader data protection rights to be formalized within GDPR.

iii. The *Google Spain* Case: Introducing a Right to Erasure

Even after the Charter of Fundamental Rights of the European Union became legally binding following the Treaty of Lisbon in 2009[35], no European policies included formal provisions regarding the right to erasure. The right, also commonly referred to as the right to be forgotten, stems from the belief that individuals have the right to 'determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past'[36]. In practice, proponents of the right to erasure believe that individuals should have the right, for example, to compel companies like Google, Inc. to remove their personal information from search list results. Opponents fear that broad delisting powers break with international norms (since comprehensive delisting would impact search results in all countries)[37] and threaten free speech around the world (since delisting could censor legitimate media coverage and impede online research efforts)[38].

Despite its absence within European regulations, the right to erasure nevertheless found legal inroads through *Google Spain v. AEPD and Mario Costeja González* (2014)[39]. In 2009, Mario Costeja González requested that *La Vanguardia*, a Spanish newspaper, remove two announcements that described his prior social security debts from Google search results. After *La Vanguardia* refused, Costeja made the same request to Google Spain and filed a formal

[35] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C306/01.
[36] Alessandro Mantalero, 'The E.U. Proposal for a General Data Protection Regulation and the roots of the "right to be forgotten"', *Computer Law & Security Review,* 29/3, 229-23 (2013).
[37] Natasha Lomas, 'Google back in court arguing against a global right to be forgotten'. [Website], (2018), Tech Crunch. <https://techcrunch.com/2018/09/11/google-back-in-court-arguing-against-a-global-right-to-be-forgotten/>.
[38] Owen Bowcott, '"Right to be forgotten" could threaten global free speech, say NGOs'. [Website], (2018), The Guardian. <https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos>.
[39] See 'Google Spain SL v. Agencia Española de Protección de Datos' (2014) 128 Harv. L. Rev. 735.

complaint with Spain's national data protection authority, the Agencia Española de Protección de Datos (AEPD), which held that Google was required to delist the announcements. Google appealed the decision before the Audiencia Nacional, Spain's highest court, but the proceedings were stayed due to a ruling by the Court of Justice of the European Union (CJEU). The ruling held that:

1. an internet search engine operator (such as Google) is responsible for personal data that it processes but which appear on third-party sites; and

2. individuals may request that their personal data be delisted from search engine results.

Three aspects of the *Google Spain* ruling warrant particular attention:

First, the defendant, Google, Inc. supported by the Advocate General, claimed that companies like search engine operators, which aggregate data hosted on third-party websites 'without effecting a selection between personal data and other information', could not be described as data controllers under the Data Protection Directive[40]. By following the precedent laid out in *Bodil Lindqvist v Åklagarkammaren i Jönköping* (2003)[41], the CJEU ruled against this interpretation, finding that Google Inc. and other data aggregators like them were data controllers and thus liable under the Data Protection Directive. Google, Facebook, and myriad other sites that aggregate content thus became liable to data erasure requests like those made by Costeja.

Second, the CJEU held that, for the purposes of data erasure requests, Google Inc., based in the United States, and its Spanish subsidiary, Google Spain, constituted a single economic unit[42]. In so unifying Google and its subsidiaries, the *Google Spain* ruling extended European data protection rights globally so long as personal data was processed, in part, by a subsidiary or branch within the E.U. Although the *Google Spain* ruling fell short of recognizing full extraterritorial enforcement—foreign entities become liable only when they extend into the E.U.—it nonetheless introduced a precedent for extraterritorial enforcement of European data protection rights.

[40] Case 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECR 317.
[41] The *Lindqvist* ruling found that the act of referring to or identifying persons on a website constitutes processing their personal data under the Data Protection Directive; Case 101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971.
[42] See Opinion of Advocate General Niilo Jääskinen, Joined Case 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECR 317.

Third, even as the *Google Spain* ruling interpreted the obligations of companies like Google broadly in processing data erasure requests, the CJEU did not interpret the Data Protection Directive to provide a broad right to erasure[43]. Rather, the court held that data erasure requests are valid only when the processing of data is inaccurate, inadequate, irrelevant, or excessive[44].

While the *Google Spain* ruling introduced many of the legal interpretations that E.U. policymakers later used to formulate a right to erasure under GDPR, it did so within the limited context of existing regulations. As a result, many of the broader implications of *Google Spain*'s expansive interpretation of data protection rights—the issues of territoriality and commercial feasibility now being raised under GDPR—were left unexplored until these data protection rights were formalized within GDPR.

[43] Case 131/12 (n 40).
[44] *Ibid* 638; this interpretation follows from Article 6(1)(e) and (f) of the Data Protection Directive, see European Union, 1995.

II. THE E.U. GENERAL DATA PROTECTION REGULATION

II.I. THE DEVELOPMENT OF GDPR

In 2010, the European Commission consulted with the European Data Protection Supervisor (EDPS) on potential updates to European data protection policies under the 1995 Data Protection Directive. The resulting Communication, 'A comprehensive approach on personal data protection in the European Union', outlined the Commission's approach to its review of E.U. legal protections for personal data in light of the rapid pace of globalization and technological innovation[45]. It was, in short, the beginning of a multi-year push to update data protection policies which ultimately resulted in GDPR.

In 2014, after gathering input from the European Commission, EDPS, and the Article 29 Working Party[46], the European Parliament (EP) voted to adopt GDPR with 621 votes in favour, 10 against, and 22 abstentions[47]. Then, in 2016, GDPR was enacted as Regulation (EU) 2016/679 with its application delayed until 25 May 2018[48], formally repealing and replacing the 1995 Data Protection Directive. Within GDPR Article 17, the EP enshrined a broad right to erasure within European law. GDPR also established the European Data Protection Board (EDPB) which includes representatives from the national data protection authorities and the EDPS and works with the national data protection authorities to apply data protection regulations.[49]

The two-year delay in applying GDPR was designed to provide firms and governments with time to assess and adopt compliance procedures. However, without compliance with data erasure requests mandated until 2018, few firms introduced extensive compliance procedures prior to the 2018 deadline. Instead, some firms—most notably Google—have chosen to devote resources

[45] Commission, 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final.
[46] The independent European working party formed to deal with 'issues relating to the protection of privacy and personal data until 25 May 2018', when GDPR was implemented.
[47] European Parliament Resolution of 12 March 2014 on the 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), COM (2012) 0011.
[48] Regulation (E.U.) 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] OJ L 119, 1-88.
[49] European Data Protection Board, 'About EDPB'. [Website], (2019), European Data Protection Board. <https://edpb.europa.eu/about-edpb/about-edpb_en>.

to litigation aimed at limiting or reverting their compliance obligations under GDPR Article 17[50]. Without clear guidance on proper compliance procedures and major litigation attempting to reduce compliance obligations, firms have had to develop compliance strategies amid major uncertainty surrounding both the costs and limitations of compliance under GDPR Article 17. These compliance challenges have only grown in the years since 2016, as growing data erasure requests under GDPR Article 17 and growing litigation regarding the extraterritorial scope of GDPR enforcement strain firms' budgets and muddle interpretations of the right to erasure under GDPR[51].

II.II. GDPR ARTICLE 17: THE RIGHT TO ERASURE

GDPR Article 17 gives individuals (or 'data subjects') the right to have personal data erased from internet search results and other data controllers or processors[52]. It is not an immutable right, however. GDPR Article 17 stipulates that at least one of the following conditions must apply for an individual to have the right to obtain erasure from a data controller or processor):

- 'the personal data is no longer necessary for the purpose [for which it was originally collected or processed];
- [the data controller is] relying on consent as [its] lawful basis for holding the data, and the individual withdraws their consent;
- [the data controller is] relying on legitimate interests as [its] basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- [the data controller is] processing the personal data for direct marketing purposes and the individual objects to that processing;

[50] See *NT1 & NT2 v. Google LLC* [2018] EWHC 799 (QB).
[51] Samuel Gibbs, 'EU to Google: expand 'right to be forgotten' to Google.com'. [Website], (27 November 2014), The Guardian. <https://www.theguardian.com/technology/2014/nov/27/eu-to-google-expand-right-to-be-forgotten-to-googlecom>.
[52] Defined in GDPR Article 4 as the 'natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. Companies, from social media platforms to banks, who collect personal data are classified as data controllers.

- [the personal data have been unlawfully processed];

- [the personal data must be erased for compliance with a legal obligation in European Union or member state law to which the controller is subject];

- [the personal data have been collected] to offer information society services to a child'[53].

This final point introduces a key provision that should be acknowledged: an emphasis on the importance of data protections for children. GDPR Article 17 implicitly encourages data controllers to give particular weight to data erasure requests for data provided by or about a child[54] since a child may not have been fully aware of the risks inherent in divulging personal information online at the time of consent and can more easily be taken advantage of.

GDPR Article 17 also compels data controllers to inform others organizations[55] about a request for data erasure under two circumstances:

1. 'the personal data has been disclosed to others; or

2. the personal data has been made public in an online environment (for example, on social networks, forums, or websites)'[56].

If data has been disclosed to others, the relevant controller has a duty to inform these recipients of the request for erasure unless doing so is 'impossible' or would require 'disproportionate effort'[57]. The controller also has a duty to divulge to the requestor which other organisations may

[53] Article 17, EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1.
[54] Importantly, this caveat holds for data subjects who are no longer children so long as the data request concerns information provided when they were children. See Information Commissioner's Office (ICO), 'Right to erasure'. [Website], (2019), Information Commissioner's Office. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/>.
[55] The GDPR defines 'others' as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
[56] Article 17 (n 53).
[57] *Ibid.*

hold their data. If the data has been made public through social networks, online forums, or similar online sites, the data controller must take 'reasonable steps' to inform other controllers processing the data to erase links, copies, and replication of the data. Given the wide dispersal of data in these domains, comprehensively notifying all possible recipients of the data may prove near impossible, hence consideration of what constitutes 'reasonable steps' focuses on the type of technology or third-party site in question as well as the cost of compliance[58].

When removing personal data under GDPR, controllers are currently required to remove data from both live systems and back-up systems[59]. Because live systems update immediately when changes are made, removing data from live systems is fairly straightforward for data controllers. Removing data from back-up systems, on the other hand, may not be technically feasible for many data controllers; these systems often have built-in time delays that block updating until old data is overwritten. In such cases, the controller must put the back-up data 'beyond use'—that is to say, they must ensure that the data cannot be used for any purpose by anyone until they are erased in line with an established schedule. While these steps should reduce the risk of personal data being abused during the interim period, they place significant trust in the controller to both implement sufficient delisting procedures and act in good faith without substantial oversight or verification by regulators or requestors. If data cannot be immediately erased, the controller has a duty to clearly communicate to the requestor what will happen to their data in respect of back-up systems[60], but regulators have not compiled sufficient evidence to determine if data controllers are complying with this requirement.

The GDPR's right to erasure also provides several grounds for when a request can be refused. These are:

- 'to exercise the right of freedom of expression and information;

[58] Clearly, the threshold for 'disproportionate effort' and 'reasonable steps' is subjective, and in practice depends significantly on controllers being willing to act in the general spirit of the legislation to be effective. The ambiguity of compliance standards laid out within GDPR Article 17 create a dichotomy within firm compliance: data controllers are both empowered to enforce data erasure obligations how they wish and obliged to carry the large and growing costs of that compliance, leading to greater dominance by large and wealthy data controllers. This consequence of GDPR Article 17 is discussed in more detail below.
[59] Article 17 (n 53); also see ICO (n 47).
[60] Eugenia Politou, Alexandra Michota, Efthimios Alepis, Matthias Pocs, & Constantinos Patsakis, 'Backups and the right to be forgotten in the GDPR: An uneasy relationship', *Computer Law & Security Review,* 34/6, 1247-1257 (2018).

- to comply with a legal obligation;

- for the performance of a task carried out in the public interest or in the exercise of official authority;

- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

- for the establishment, exercise or defence of legal claims.'[61]

Importantly, the right to erasure does not apply under two conditions:

1. '[when data processing is required] for public health purposes in the public interest (such as protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

2. if the processing is necessary for the purposes of preventative or occupational medicine (such as where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). [However, this] only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (such as a health professional).'[62]

Data controllers may also refuse a request for erasure if it is 'manifestly unfounded or excessive', taking into consideration whether the request has been made repeatedly.[63] In these circumstances, the controller may request a 'reasonable fee' to cover the administrative costs of complying with the request or may outright refuse to comply with the request[64]. If a controller decides to refuse a request or ask for a fee, they must inform the individual as soon as possible

[61] Article 17 (n 53).
[62] *Ibid.*
[63] *Ibid.*
[64] *Ibid.*

and within one month of receiving the request, making sure to provide reasons for the decision and highlighting the individual's right to make a complaint to the relevant supervisory authority and recourse to legal action to remedy any dispute.

Failure to comply with Article 17 may result in administrative fines, which may be as severe as €20 million or 4% of annual global revenue from the previous financial year[65], and temporary or permanent bans on processing data[66].

II.III. EVALUATING GDPR ARTICLE 17

i. RULES-BASED VERSUS PRINCIPLES-BASED REGULATION

Section II.II highlights a number of Article 17 provisions meant to guide firm compliance and government-side regulation. These provisions were designed to provide certain and enforceable guidelines that (1) citizens can follow to exercise their newfound right to erasure and (2) corporations can follow to comply with right to erasure requirements. While GDPR Article 17 does include a variety of explicit guidelines and procedural requirements—i.e. rules-based regulations—most of the stipulations found within GDPR define broad principles of regulation and implicit regulatory schemes rather than explicit protocols—i.e. principles-based regulation (PBR). For example, GDPR Article 5 sets out seven key principles derived from the Data Protection Act of 1998[67]:

1. Personal data should be 'processed lawfully, fairly and in a transparent manner',

2. Personal data should be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes',

[65] Matt Burgess, 'What is GDPR? The summary guide to GDPR compliance in the U.K.'. [Website], (2019), Wired. <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>.
[66] Article 58(2)(f), *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.
[67] U.K. Data Protection Act 1998, c 29.

3. Data controllers and processors should request only those personal data that are 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed',

4. Personal data kept by data controllers should be kept 'accurate and, where necessary, up to date',

5. Personal data should be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed',

6. Personal data should be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage', and

7. Data controllers should be 'responsible for, and be able to demonstrate compliance with' all accountability requirements[68].

Principles-based regulation (PBR) is a well-researched regulatory approach, with both strengths and limitations[69]. The main benefits of PBR are its flexibility and its shift from strict procedural compliance to substantive regulatory compliance[70]. As technological progress continues to accelerate, for example, traditional forms of regulation may not be enough to protect user data from new technologies and processing techniques[71]; firms may find new uses for previously uncollected personal data, or new technologies may generate new forms of personally-identifiable data that were not previously protected[72]. Similarly, requiring firms to comply with principles

[68] Article 5, *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.
[69] See, e.g., Julia Black, 'Forms and paradoxes of principles-based regulation', *Capital Markets Law Journal,* 3/4, 425-457 (2008); Julia Black, 'The rise, fall and fate of principles based regulation'. [Working Paper], (2010), London School of Economics and Political Science, Law Department. <http://eprints.lse.ac.uk/32892/1/WPS2010-17_Black.pdf>.
[70] Black, 'Forms and paradoxes of principles-based regulation' (n 62).
[71] See Declan Butler, 'Tomorrow's technological change is accelerating today at an unprecedented speed and could create a world we can barely begin to imagine', *Nature* 530, 399 (25 February 2016).
[72] For example, the creators of Roomba, the robotic vacuum, revealed in 2017 that their robots collected spatial data about users' homes. Maggie Astor, 'Your Roomba may be mapping your home, collecting data that could be shared'. [Website], (25 July 2017), New York Times. <https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.>

forces firms to shift their compliance procedures away from 'box-ticking' and compliance minimisation[73]. However, PBR is also vulnerable to a number of limitations, including:

1. Failure to provide adequately precise regulatory guidance for 'edge case' scenarios;

2. Uncertainty surrounding enforcement behaviour can lead firms to either adopt conservative behaviour or attempt to avoid enforcement altogether; and
3. Uncertainty surrounding enforcement can also lead regulators to forego enforcement of complex or politically volatile matters[74].

Because GDPR Article 17 is, at its core, a principles-based regulatory approach, U.K. firms and regulators alike have substantial flexibility in determining how exactly to comply with and enforce right to erasure requirements, respectively[75]. This has led to many U.K. firms to adopt conservative firm behaviours that provide greater protection and transparency to citizens[76], but it has also enabled many firms to avoid, reduce, or delay Article 17 compliance; an estimated 70% U.K. organisations still fail to comply with GDPR requirements more than a year after the regulations came into force[77].

To ensure that citizens' digital rights are protected under a PBR scheme and amid rapid technological change, regulators must have tools flexible enough to apply to numerous regulatory environments—even those that may not yet exist[78]. By establishing principles to guide local regulation rather than a set of established rules and procedures, GDPR reflects an attempt to provide policymakers with flexible, adaptable regulatory tools. However, it has also led to comparatively lax enforcement. While certain large firms have faced severe fines for their failure to comply with GDPR requirements[79], many firms have faced no repercussions for their compliance shortfalls to date[80].

There are several reasons for U.K. regulators' enforcement behaviour. To determine whether data controllers are complying fully with GDPR right to erasure requirements, regulators need

[73] Black, 'Forms and paradoxes of principles-based regulation' (n 62).
[74] *Ibid.*
[75] Article 5 (n 68).
[76] Deloitte (n 6).
[77] Talend (n 9).
[78] See Butler (n 64).
[79] See Adam Satariano, 'Google is fined $57 million under Europe's data privacy law'. [Website], (21 January 2019), New York Times. <https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html>.
[80] Talend (n 9).

more information—often information about the kinds of data firms keep and kinds of processing procedures that firms use, which few firms are willing to reveal[81]—than they currently have access to[82]. Further, since most individuals making data erasure requests may not have the time and financial resources to contest the denial of a data erasure requests—especially when that request is denied by a large data controller like Google—the current regulatory environment under GDPR provides few protections and little governmental arbitration for these requests, leaving both the interpretation of and compliance with GDPR Article 17 primarily to data controllers.

Another challenge to the enforcement and evaluation of right to erasure provisions under GDPR comes with the ambiguity of what forms data erasure requests can take. GDPR Article 17 doesn't specify that data erasure requests must be made in writing, meaning verbal requests—even those made to employees of a data controller uninvolved with GDPR compliance procedures—may hold legal weight. Additionally, requests do not have to explicitly quote GDPR Article 17, meaning that organisations must take particular care to ensure that employees who deal with the public are adequately trained to recognise and accurately record requests for erasure, particularly when these requests are made verbally. Recording the details of requestors, keeping a log of verbal requests, and ensuring both the employee and requestor have the same understanding of what the request entails before it is actioned are all suitable steps controllers can take to avoid the risk of complaints or litigation arising from misunderstandings. However, data controllers—especially large firms and their subsidiaries—may not be able to feasibly comply with all verbal requests, considering the myriad costs associated with tracking requests, training employees, and informing all parties involved of what actions have been taken—as well as the costs associated with increased requests processing.[83]

In addition, data controllers are required to act as quickly as possible—but at the latest within one calendar month from the day the request is received—to process requests and, if necessary, remove all relevant personal data. If the request is complex (or if several requests are received from the same individual), controllers are permitted to extend the response time by a maximum of two months, provided they inform the individual about the reasons for the extension as soon

[81] See CEBR & SAS, 'The value of Big Data and the Internet of Things to the UK economy'. [Report], (2016), CEBR. <https://www.sas.com/content/dam/SAS/en_gb/doc/analystreport/cebr-value-of-big-data.pdf>; CtrlShift & U.K. Department for Digital, Culture, Media & Sport, 'Data Mobility: The personal data portability growth opportunity for the UK economy'. [Report], (2018), CtrlShift & U.K. Department for Digital, Culture, Media, & Sport. <https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf>
[82] *Ibid.*
[83] *Ibid.*

as practicable and at the latest within one month of receiving the request. Controllers may also ask for identification to check the authenticity of the request if in doubt; they do not need to process the request until such proof is received.[84]

Taken together, these limitations and GDPR's PBR approach to data protection suggest that, while GDPR Article 17 may provide U.K. policymakers with robust and adaptable regulatory tools, these tools may not be effective without a slew of complementary, rules-based regulations like court rulings and published guidance[85]. U.K. regulators therefore face a dilemma: without clearer, rules-based regulations, regulators today lack the ability to effectively enforce all GDPR requirements, but developing strict, rules-based regulations may significantly restrict their ability to adapt to changes in the U.K.'s data ecosystem[86]. Consequently, it is incumbent on policymakers and regulators to take additional measures where possible to strengthen their own capacity to enforce GDPR effectively and find ways to support organizations as they continue working towards compliance.

[84] *Ibid.*
[85] Black, 'The rise, fall and fate of principles based regulation' (n 62).
[86] Black, 'Forms and paradoxes of principles-based regulation' (n 62); *ibid.*

III. U.K. IMPLEMENTATION AND ENFORCEMENT

III.I. IMPLEMENTING GDPR IN THE U.K.

While E.U. member states were able to form their own regulatory approaches to the Data Protection Directive of 1995[87], GDPR is a binding act that requires all member states to follow the same regulations[88]. Therefore, GDPR requirements automatically came into force in the U.K. at the same date as in other E.U. member states—25 May 2018. However, GDPR did enable member states to determine how certain provisions applied locally[89]. In the U.K., these local provisions were enshrined in the Data Protection Act 2018[90] (DPA 2018), which achieved royal assent on 23 May 2018 and included provisions to:

1. Extend GDPR to domestic U.K. law to enable regulators to use domestic enforcement tools;

2. Extend GDPR data processing provisions to areas that fall outside the scope of E.U. law (e.g. immigration and national security); and

3. Formalize provisions required to maintain ongoing ICO duties and develop processes to handle the interaction between U.K. data protection laws and GDPR[91].

Together, GDPR and DPA 2018 were designed to facilitate compliance and regulation within the U.K.'s existing, domestic regulatory structure. As discussed in Sections II.III and III.II, however, GDPR's principles-based regulations and the introduction of novel compliance requirements have caused several enforcement and compliance challenges in the year since GDPR and DPA 2018 went into effect.

[87] Directive (EC) 95/46 (n 24).
[88] European Union, 'Regulations, directives and other acts'. [Website], (2019), European Union. <https://europa.eu/european-union/eu-law/legal-acts_en>.
[89] Information Commissioner's Office, 'Data Protection Act 2018'. [Website], (2019), ICO. <https://ico.org.uk/for-organisations/data-protection-act-2018/>.
[90] Data Protection Act 2018, c 12.
[91] *Ibid.*

III.II. ARTICLE 17 COMPLIANCE IN THE U.K.

i. Compliance Challenges

Complying with the right to erasure (along with the other provisions of the GDPR) imposes significant costs on organisations, both large and small[92]. In addition to the appointment of a 'Data Protection Officer' responsible for GDPR compliance, collectors must provide comprehensive training to educate both existing staff and new hires, imbed new compliance processes into existing business operations, and develop or purchase new software tools to facilitate efficient and expeditious compliance. These requirements have generated significant increases in firm data protection and compliance budgets since GDPR was brought into force, as well as increased legal fees raised to litigate compliance obligations under GDPR[93].

These costs are clearly showcased within the IAPP-EY Annual Privacy Governance Report 2018, which surveys a representative sample of 550 data protection professionals from various firms across Europe and other developed economies[94]. Firms are currently spending an average of U.S.$1.3 million annually to respond to GDPR, with an average of ten additional staff hired to deal exclusively with data protection issues.[95] Consequentially, data protection issues appear to be gaining much more prominence within operational guidelines, with 44% of organisations elevating the position of Data Protection Officer or other similar position within their corporate hierarchy.[96] Privacy by design principles, such as improving the accuracy of data capture and storage, limiting data processing, and minimising the quantity of data held at any one time, have increasingly become embedded into the development and maintenance of digital products and services.

Despite this uptick in compliance costs, 56% of firms who are subject to GDPR have stated that their compliance procedures fall far short of GDPR requirements—or even that they will never

[92] IAPP and EY, 'IAPP-EY Annual Privacy Governance Report 2018'. [Website], (2018), IAPP. <https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf>.
[93] Oliver Smith, 'The GDPR Racket: Who's Making Money From This $9bn Business Shakedown'. [Website], (2018), Forbes. <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/>
[94] IAPP and EY, 'IAPP-EY Annual Privacy Governance Report 2018'. [Website], (2018), IAPP. <https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf>.
[95] *Ibid.*
[96] *Ibid.*

be able to fully comply. Of all the requirements under GDPR, those surrounding the right to erasure are considered by these firms to be the most challenging to comply with. (See Figure 1.)[97] Although firms still struggle to comply with the right to erasure, however, they appear to be learning how to best accommodate the right to erasure within their business operations, as evidenced by a slight decline in perceived difficulty from 2017 to 2018. Interestingly, U.S. firms report greater difficulty in complying with the GDPR provisions, with the right to erasure reported as 6.6 out of 10 in comparison to the overall average of 5.8. This may reflect the legal and jurisdictional challenges that foreign firms face when attempting to comply with GDPR provisions, as well as ongoing technical challenges imposed by the requirement to permanently delete individuals' data. Additionally, across both Europe and the U.S., respondents within the financial services sector appear to be more concerned with compliance to the right to erasure than other sectors.[98]

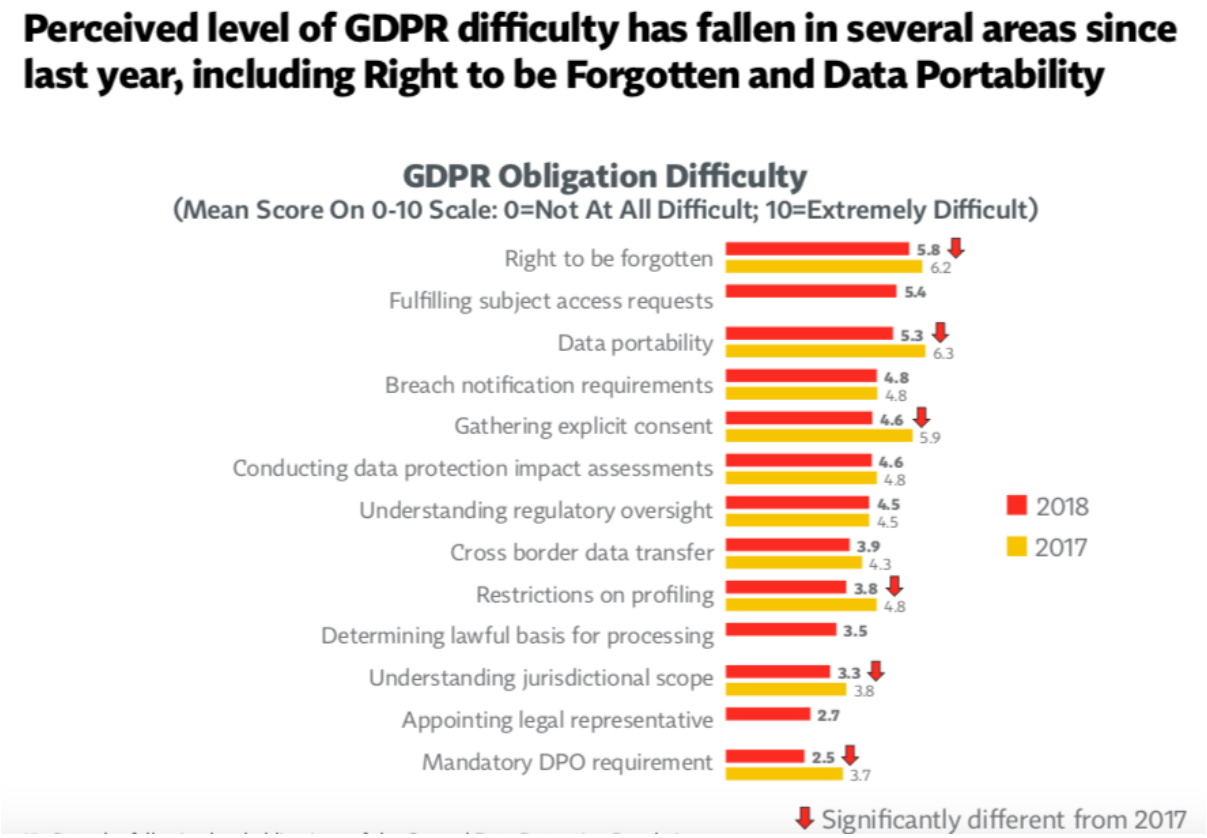
ii. Compliance Case Study: Google

Google, one of the world's largest data controllers and the subject of data erasure obligations going back to the *Google Spain* case in 2014, serves as a particularly enlightening case study of what GDPR compliance entails today. Following the *Google Spain* ruling, Google developed internal procedures to evaluate data erasure requests made by E.U. citizens who identify search engine results about themselves that are 'irrelevant, outdated or otherwise objectionable'[99]. By the end of 2018, Google had received around 723,000 requests, 44% of which it considered legitimate[100]. Celebrities, politicians, and government officials have dominated requests for delisting[101]. Google noted that 'frequent requesters', often 'law firms and reputation management services', made up only 15% of all requests; just over half of all requests came from just three countries: France, Germany and the U.K.[102] Despite the number of data erasure requests,

[97] *Ibid.*
[98] *Ibid.*
[99] Julia Powles & Enrique Chaparro, 'How Google Determined Our Right to be Forgotten'. [Website], (18 February 2015), The Guardian. <https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search>.
[100] Michèle Finck, 'Google v CNIL: Defining the Territorial Scope of European Data Protection Law'. [Webiste], (16 November 2018), Oxford Business Law Blog. <https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law>.
[101] James Doubek, 'Google Has Received 650,000 'Right to Be Forgotten' Requests Since 2014'. [Webiste], (28 February 2018), NPR. <https://www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014?t=1552234260819>.
[102] *Ibid.*

however, only about 1% of requestors who had their requests denied appealed those decisions to national data protection authorities[103].

Figure 1: GDPR provisions' obligation difficulty survey results[104]



The costs imposed by the right to erasure on data controllers are high. Google noted that the 'logistically complicated' process of evaluating requests by weighing them against public interest is conducted on a 'case-by-case basis', requiring far more time and resources than a broad

[103] Jacques de Werra, 'ADR in Cyberspace: The Need to Adopt Global Alternative Dispute Resolution Mechanisms for Addressing the Challenges of Massive Online Micro-Justice', *Swiss Review of International & European Law 2016*, 289-306 (21 November 2016).
[104] IAPP and EY, 'IAPP-EY Annual Privacy Governance Report 2018'. [Website], (2018), IAPP. <https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf>.

procedural approach[105]. In assessing public interest, a multitude of factors—like whether the content pertains to a requester's professional life, a past crime, public life, or whether it is self-authored or is journalistic in nature—have to be examined by employees. The process is costly in terms of time and manpower, requiring Google and other, similarly-positioned data controllers to make vast investments into new compliance procedures. Moreover, despite the investments already made by Google since 2014, though, information technology professionals expect that GDPR compliance will require even more: over 80% of those surveyed in a 2017 study by Dimensional Research anticipated GDPR-related expenditure would amount to at least U.S.$100,000[106].

Google's expenditures are not unique, either. To comply with GDPR today, E.U. and U.S. companies spend, on average, an estimated €200 billion and U.S.$41.7 billion, respectively[107]. According to consultants at Ernst & Young, the world's 500 biggest corporations are on track to spending a total of $7.8 billion to comply with GDPR; besides appointing teams of liaison personnel to work with E.U. regulators, many large companies have designated data protection officers responsible for compliance[108]. Microsoft, for instance, has 300 engineers working to ensure its software is GDPR-compliant[109].

Rather than incorporate potentially costly GDPR compliance procedures into their business models, many tech companies have chosen to challenge Article 17 requirements in court. Google, for its part, has repudiated any and all charges by requestors and regulators that Google's data processing algorithms are at fault. Google's Executive Chairman, Eric Schmidt, and Chief Legal Counsel, David Drummond, view Google search as merely an online 'card index'[110]. In fact, in the Argentinian case of *Da Cunha v. Yahoo/Google* (2010), Judge Patricia Barbieri observed that search engines could not be held responsible for the content individuals and entities decided to publish on their own websites; the fact that search engines catalogued those

[105] Charles Arthur, 'Google Faces Deluge of Requests to Wipe Details from Search Index'. [Website], (15 May 2014), The Guardian. <http://www.theguardian.com/technology/2014/may/15/hundreds-google-wipe-details-search-index-right-forgotten>; Doubek (n 70).
[106] Chris Babel, 'The High Costs of GDPR Compliance'. [Website], (7 November 2017), UBM. <https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263>.
[107] See 'GDPR Compliance Cost Calculator'. [Website], (2019), Gigacalculator. <https://www.gigacalculator.com/calculators/gdpr-compliance-cost-calculator.php>.
[108] Kahn et al. (n 5).
[109] *Ibid.*
[110] Powles & Chaparro (n 68).

sites and recommended links were insufficient to establish causation with respect to injury, according to the judge[111]. She quoted Section 230 of the U.S. Communications Decency Act and a similar provision in the E.U.'s 2000 Electronic Commerce Directive, reiterating that search engines could not be held responsible. Barbieri also invoked Google's own Terms of Service, which expressed that Google was not responsible for content on third party websites, as well as Google's compliance with the notice and take-down provisions of the U.S. Digital Millennium Copyright Act (1998). Judge Diego C. Sanchez, however, disagreed and asserted that search engines are not simply passive carriers of information, but active participants in attracting attention to particular sites while disregarding others[112]. As such, he argued that search engines could cause harm to individuals whose personal information is reflected in search outcomes. At a broader level, Google and other tech companies are beginning to acknowledge the role that they play in disseminating harmful information and have taken down content in some cases.[113]

Crucially, Article 17 compliance requirements may continue to impact the U.K.'s digital competition policy as well. Because GDPR Article 17 places the burden of managing right to erasure requests on digital firms, larger firms like Google, which have the resources to quickly develop compliance procedures or respond to legal challenges, are better positioned than smaller firms to interpret and implement GDPR for their businesses.[114] To ensure industry-wide compliance with GDPR Article 17 without exacerbating anticompetitive practices, U.K. regulators will need to consider policy solutions that do not disproportionately affect less-established firms.[115] Admittedly, all firms should have complied by the time GDPR officially went into effect, but in practice, confusion surrounding GDPR made that improbable, especially for small businesses.[116]

---

[111] *Virginia Da Cunha v. Yahoo de Argentina S.R.L. and Google* (2010) Expte. Nº 99.620/2006, Recurso Nº541.482. Juzgado Nº 75; Edward L. Carter, 'Argentina's Right to be Forgotten' (2014). *Emory International Law Review,* 27, 23-38.

[112] *Ibid.*

[113] Natasha Lomas, 'YouTube is now taking down more videos of known extremists — in major policy change'. [Website], (14 November 2017), TechCrunch. <https://techcrunch.com/2017/11/14/in-major-policy-change-youtube-is-now-taking-down-more-videos-of-known-extremists/>

[114] Mark Scott, Laurens Cerulus and Steven Overly, 'How Silicon Valley gamed Europe's privacy rules'. [Website], (22 May 2019), Politico. < https://www.politico.com/story/2019/05/25/how-silicon-valley-gamed-the-worlds-toughest-privacy-rules-1466148>

[115] Daisuke Wakabayashi and Adam Satariano, 'How Facebook and Google Could Benefit From the G.D.P.R., Europe's New Privacy Law'. [Website], (23 April 2018), The New York Times. <https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html>

[116] Rob Knight, 'GDPR: Small business owners still 'clueless' about data protection rules, study claims'. [Website], (12 December 2018), The Independent.

iii. Considering Technical Compliance Solutions

To address the high costs of GDPR compliance, data controllers are turning to digital innovations to 'automate; compliance with GDPR's right to erasure in a secure and scalable way. Security researchers from the Helmholtz Center for Information Security (CISPA), Saarland University, and the University of Auckland have developed a software prototype that validates data erasure requests within seconds and allows users to automatically locate and tag their personal information on the web using text and image recognition. Called Oblivion, the digital platform handles up to 278 requests per second[117]. It not only verifies the personal identity of users and helps them file requests with the relevant URLs securely, but it also checks the websites from which users want data removed and tags user references before sending them to Google[118]. The automated eligibility proof that Oblivion provides precludes unwarranted censorship; links from search results can only be removed by legitimately-affected individuals themselves. Still, the final decision regarding data erasure requests rests in the hands of data controllers' employees; data erasure requests relating to matters of public health and public interest, for example, still need to be handled by employees of data controllers on a case-by-case basis. Oblivion merely automates and expedites certain compliance procedures.

The introduction of automated compliance procedures highlights the need for greater oversight of data controllers processing requests. Following the *Google Spain* ruling and without greater clarity within GDPR Article 17, data controllers currently function as the implementers and enforcers of GDPR right to erasure provisions, taking over a function traditionally reserved for state regulators. In this new digital regime, private search engine operators become responsible not only for judging the relevance of and public right to information containing personal data, but also for censoring those they consider unlawful. Individual appeals to public authorities are possible, but rare, leaving data controllers—especially large multinational entities like Google and Microsoft—with immense freedom to mould the interpretation and enforcement of GDPR Article 17[119]. It does not help that the entire delisting process is largely opaque. European courts

[117] Jordan Pearson, '"Oblivion" Is the Software That Could Automate the "Right to Be Forgotten"'. [Website], (22 June 2015), Vice. <https://motherboard.vice.com/en_us/article/4x393p/oblivion-is-the-software-that-could-automate-the-right-to-be-forgotten>.
[118] Milivoj Simeonovski, Fabian Bendun, Muhammad Rizwan Asghar, Michael Backes, Ninja Marnau, & Peter Druschel, 'Oblivion: Mitigating Privacy Leaks by Controlling the Discoverability of Online Information' in *13th International Conference on Applied Cryptography and Network Security* (ACNS 2015).
[119] Finck (n 69).

have only set vague standards for how delisting should occur; in the *Google Spain* ruling, for example, the court held that the examination of a request should strike a 'fair balance' between the general interests of internet users and the 'fundamental rights' of a requester.[120] It is this interpretational ambiguity that has left data controllers confused regarding enforcement procedures for the right to erasure.

III.III. ENFORCING ARTICLE 17 COMPLIANCE

i. Ensuring Accountability and Enforcement

The problem of accountability arises when private companies take on the traditionally judicial role of making decisions regarding the interpretation and implementation of the law. When Google acceded to the request from a British doctor to have fifty links removed on past botched medical procedures because they contained his personal data, the public voiced their outrage for the censorship of information that can cause people to make uninformed decisions[121]. Without oversight, search engine operators have no reason to strictly abide by compliance obligations, raising fears that the delisting process may make search engine results biased, patchy, or otherwise censored without explanation.

The precedent set under GDPR will also dictate how future governments, both within Europe and abroad, approach data protection rights in the future. Google's CEO, Larry Page, expressed concerns that the right to erasure may be 'used by other governments that aren't as forward and progressive as Europe to do bad things'[122]. Delisting has been conducted without disclosing internal processes, removal criteria, or the way cases have been prioritised[123]. By putting together an 'advisory council' of experts, Google has insulated its practices from outside oversight with a veneer of legitimacy and accountability. Little is known not only about the information that is delisted from search results, but also the guidelines used by major data controllers to balance issues of individual privacy and data protections, freedom of expression, and the free access to information. Additionally, while delisting results on a search engine does not entail deleting

[120] Case 131/12 (n 40).
[121] David Payne, 'Google, Doctors, and the "Right to be Forgotten"'. [Website], (6 January 2015), The BMJ. <https://www.bmj.com/content/bmj/350/bmj.h27.full.pdf>.
[122] Samuel Gibbs, 'Google Hauled in by Europe over "Right to be Forgotten" Reaction'. [Website], (24 July 2014), The Guardian. <https://www.theguardian.com/technology/2014/jul/24/google-hauled-in-by-europe-over-right-to-be-forgotten-reaction>.
[123] Powles & Chaparro (n 68).

information from the original website, in practice, it does make that information harder to access. Data controllers like Google benefit from these informational imbalances between firms and regulators, rarely revealing their processes and procedures to regulators and contesting regulatory obligations in court. To preserve the data protection rights of British citizens, U.K. regulators will need to constantly educate themselves on new technological developments and develop processes to facilitate oversight. However, in the face of a broader digital skills gap, they may not have the necessary resources to follow through—at least in the short-term.[124]

ii. Territoriality and GDPR Enforcement

The Force of GDPR Abroad

As de facto interpreters and enforcers of GDPR, data controllers, many of whom operate outside of the E.U. as well, become de facto exporters of E.U. law abroad as well[125]. In so exporting GDPR standards globally, data controllers have become tools of European 'data imperialism'—they not only enforce data protection policies within the E.U., but they mould data protection policies elsewhere as well. The spread of GDPR enforcement to non-E.U. polities raises several geopolitical concerns that have yet to be settled, many of which U.K. policymakers must be aware to minimize future trade and geopolitical conflicts.

Currently, data controllers are bound by E.U. law to remove personal data subject to Article 17 data erasure requests globally. The Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection authority, found that data protection rights were insufficiently protected when Google delisted search results only in E.U. domains, such as Google.de or Google.fr. CNIL argued that Google had to delist search results that have been designated for erasure from all domains worldwide to ensure the effective protection of data subjects' rights[126]. Google's appeal of CNIL's decision, on the basis that European authorities should not extend their own data protection rules across the globe, is presently undergoing review by the European Court of Justice (ECJ)[127].

[124] House of Commons Science and Technology Committee, 'Digital Skills Crisis – Second Report of Session 2016-17'. House of Commons (HC 270).
<https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf>
[125] Finck (n 69).
[126] *Ibid.*
[127] *Ibid.*

Indeed, data controllers may soon have to contravene the law in non-E.U. jurisdictions. In 2016, for example, E.U. and U.S. regulators jointly established the E.U.-U.S. Privacy Shield agreement to facilitate data transfers between the U.S. and E.U. member-states[128]. Under the Privacy Shield agreement, all registered businesses in the Privacy Shield are subject to EU enforcement actions under GDPR[129]. Therefore, Google is required to apply right to erasure provisions to search results accessible in the U.S. so long as they do not infringe U.S. 'constitutional rights, rights established under federal or state laws, or public policy considerations'[130]. While GDPR enforcement against non-E.U. entities without any relationship with or representation within the E.U. is unlikely, legal scholars disagree on the extent to GDPR's extraterritorial force in non-E.U. jurisdictions without comparable data protections regulations but some relevant form of diplomatic agreement with the E.U.[131]. These potential extraterritorial applications of the right to erasure raise serious concerns relating to international, cyber, and privacy law, including the degree to which the E.U. can and should regulate the global operations of foreign-based data controllers like Google and the extent to which the E.U. can restrict the locally-conceived digital rights of people outside of the European Union.

GDPR is not the first time that the E.U. has dictated the course of policy internationally. In her 2012 book, *The Brussels Effect*, Columbia Law School Professor Anu Bradford highlights 'Europe's unilateral power to regulate global markets' by externalising regulations like those regarding the right to erasure[132]:

[128] Andrus Ansip and Věra Jourová, 'Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield'. [Website], (2016), European Commission. <http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm>.
[129] See U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework Principles'. [Website], (2016). < https://www.privacyshield.gov/EU-US-Framework>.
[130] See *Matusevitch v Tenikoff* [D.D.C. 1995] 877 F.Supp. 1, 2 (US); *Mata v Am. Life Ins. Co.* [D. Del. 1991] 771 F. Supp. 1375, 1384 (US); *Abdullah v. Sheridan Square Press, Inc., No. 93CIV.2515 (LLS)* [SDNY 1994] 1994 WL 419847 (US).
[131] Mostafa al Khonaizi, 'Fines under EU GDPR in Non-EU Jurisdictions: Enforceable or Mere Reputation Risk?'. [Website], (2018), Michigan Journal of International Law. <http://www.mjilonline.org/fines-under-eu-gdpr-in-non-eu-jurisdictions-enforceable-or-mere-reputation-risk/#_ftn21>; RV Anuradha, 'India: What the European Union's Data Protection Rules Mean for Your Business'. [Website], (18 September 2018), Mondaq. <http://www.mondaq.com/india/x/737394/Data+Protection+Privacy/What+the+European+Unions+data+protection+rules+mean+for+your+business>.
[132] Anu Bradford, 'The Brussels Effect', *Northwestern University Law Review*, 107/1, 1-68 (2012).

> 'While the E.U. only regulates its internal market, multinational corporations often have an incentive to standardize their production globally and adhere to a single rule' since firms have an 'incentive to lobby their domestic governments to adopt these same standards in an effort to level the playing field against their domestic, non-export-oriented competitors'[133].

In 2012, Graham Greenleaf, now Professor of Law at the University of New South Wales, observed that over 30 non-European countries have adopted E.U.-style data protection laws:

> 'There is nothing occurring in the rest of the world which represents a coherent alternative to the spread of European-influenced data privacy standards, or even coherent resistance to the adoption of such standards'[134].

Regardless of government policies, several U.S. firms like Microsoft have already adopted GDPR provisions as their de facto data protection standards for all global operations[135]. For many non-E.U. policymakers, the choice between updating domestic laws to accommodate the E.U.'s new regulations and the risk of being excluded from a regional market of 500 million reasonably well-heeled consumers is a no-brainer. As U.K. policymakers develop their own data protection standards post-Brexit, the commercial and regulatory force of E.U. policies will likely persist, restricting what the U.K. can do to protect its citizens and attract investment in digital sectors.

Considering Global Variations in Data Protection Policies

Despite the long reach of GDPR, several regulators around the world have taken different positions on issues of data protection rights. Nearly 30% of all nations have no data protection laws; those that do often have laws incompatible with GDPR[136]. For example, U.S. courts, which

---

[133] *Ibid.*
[134] Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' *International Data Privacy Law,* 2/2, 68–92 (2012).
[135] Brad Smith, 'Privacy Authorities Across Europe Approve Microsoft's Cloud Commitments'. [Website], (9 April 2014), Microsoft. <https://blogs.microsoft.com/eupolicy/2014/04/09/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/>.
[136] William D. Eggers, Mike Turley, & Pankaj Kishnani, 'The Future of Regulation Principles for Regulating Emerging Technologies'. [Website], (19 June 2018), Deloitte Insights. <https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation/regulating-emerging-technology.html#endnote-27>.

operate under markedly weaker data privacy rights, are unlikely to locally enforce the CNIL ruling that requires Google to delist material from global search results, which stems from GDPR provisions rather than U.S. legal precedence[137].

According to Simon McGarr, the Director of Compliance Europe, a data protection consultancy, E.U. policymakers based GDPR on decades of case law defining what, exactly, constitutes personal data, as well as nuances of European political history, from its dealings with totalitarian states to the creation of the European Union[138]. Far from being a universally applicable standard for data protections, then, GDPR is a fundamentally Euro-centric conception of data protection rights—one that will more than likely be contested by firms and foreign polities as data protection procedures become more widespread. In the future, U.K. policymakers should recognize that they will also need to regularly evaluate the E.U.'s data protection provisions as GDPR evolves over time within the global context to determine what provisions are enforceable, commercially feasible, and in line with the interests of British citizens.

Even though the E.U.'s data protection policies are currently aligned with the wishes of E.U. citizens[139], there is no reason that these policies will necessarily remain within the best interest of the wider public in the future. Relying too heavily on the E.U. to set the standards for data protection rights may have adverse implications for policymakers both within the U.K. and abroad in the long-term. Enabling an extraterritorial approach to GDPR compliance without regard to local policy differences and state sovereignty also promotes a form of 'data imperialism'[140] that may cause schisms in both new and old relationships with foreign allies—many of whom will be invaluable trading partners and allies for a post-Brexit U.K.

It is critical to remember that GDPR came about as an update to and unification of European data protection laws; it was not designed to be a global standard. GDPR's provisions, coupled

[137] Lomas (n 31).
[138] Jill Petzinger, 'GDPR is the most unifying thing to happen to the E.U. in a while'. [Website], (24 May 2018), Quartz. <https://qz.com/1287872/gdpr-is-the-most-unifying-thing-to-happen-to-the-eu-in-a-while/>.
[139] See Věra Jourová, 'Data Protection: Factsheet 4. European Commission'. [Website], (2015), European Commission. <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf>.; Eggers, Kishnani, & Turley (n 95).
[140] Mark Scott & Laurens Cerulus, 'Europe's new data protection rules export privacy standards worldwide'. [Website], (31 January 2018), Politico. <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/>.

with the absence of a comprehensive regulatory approach to data protection rights outside of the E.U., has provided E.U. policymakers with immense and unanticipated authority over how personal data can be collected, used, and stored around the world. Policymakers outside the E.U. have, in turn, faced an ultimatum: either bring their local, regional, and national laws in-line with GDPR or risk being excluded from the E.U. market[141].

While the U.K. is currently operating under the GDPR and the DPA 2018, it is also important to point out that, at present, while the ICO sits on the EDPB, this will necessarily change once Brexit happens. The DPA 2018 as well as the 'extraterritorial reach' of GDPR will mean that GDPR will in practice still be effective in the U.K. after Brexit[142]. Maintaining a 'parallel' regulatory environment in the immediate future while data protections have just recently been updated should not be particularly controversial[143]; nevertheless, down the road, as updates to the GDPR are debated to meet changes in the future digital environment with continued extraterritorial reach, the U.K.'s lack of authority within the EDPB and inability to contribute to new regulations may bring about conflict with Brussels.

In the short term, though, breaking ties with the E.U. along lines of data protection rights may not be politically and economically feasible. For many smaller and less wealthy countries—and indeed even for the U.K.—the choice to abide by E.U. regulations is often one of necessity; the E.U. links potential free-trade agreements with demands that other countries adopt the region's data protection standards, and the same is true in a post-Brexit world[144]. When considering the commercial and geopolitical implications of the U.K.'s post-Brexit data protection policies, U.K. policymakers must pay particular attention to changes in E.U. data protection policies both to maintain trade and political relationships with its closest neighbours and to better evaluate when, how, and how forcefully the U.K.'s approach to data protection rights—and especially the right to erasure—should differ from those of the E.U.

[141] *Ibid.*
[142] DLA Piper, 'U.K.: GDPR Brexit Flowchart. DLA Piper'. [Website], (2018), DLA Piper. <https://blogs.dlapiper.com/privacymatters/uk-gdpr-brexit-flowchart/>.
[143] *Ibid.*
[144] Scott & Cerulus (n 99).

IV. RECOMMENDATIONS

In light of the legal and practical challenges of implementing GDPR, it is clear that more guidance and support is necessary for effective compliance, especially with Article 17. Given that GDPR's PBR approach means that it is intentionally flexible and not overly-prescriptive, recommendations to assist in this effort include process-oriented actions that will encourage compliance and strengthen technology skills and knowledge so that policymakers and data processors and controllers are better-equipped to address regulatory ambiguities and reduce uncertainty. Tackling data protection challenges at the individual level is also an important component. While these measures are not certainly not panaceas, they would be a step in the right direction in helping GDPR succeed.

IV.I. IMPLEMENT PROCESS-ORIENTED MEASURES TO ASSIST WITH ARTICLE 17 IMPLEMENTATION

First, to enhance compliance with GDPR and Article 17, more supporting services are needed to help companies, especially smaller ones, which may have less resources to devote to GDPR compliance. While the ICO has a helpline available during business hours[145] as well as extensive guidelines on GDPR compliance for companies which are useful,[146] considering the financial burden and complexity of GDPR, more assistance should be provided, especially for small and medium businesses and organizations.[147] This could be in the form of more extensive advisory services and more hands-on business assessments. Additionally, while the ICO has established a grants program under its Information Rights Strategic Plan 2017-2021 which is certainly helpful for academic research, the program focuses on innovations and technical solutions to data protection challenges[148]. Considering the expense of implementing GDPR,[149] the ICO should

[145] Information Commissioner's Office (ICO), 'Helpline'. [Website], (2019), Information Commissioner's Office. <https://ico.org.uk/global/contact-us/helpline/>.
[146] Information Commissioner's Office (ICO), 'Guide to the General Data Protection Regulation (GDPR)'. [Website], (2019), Information Commissioner's Office. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>.
[147] Pavol Magic, 'How Small Businesses Can Survive in the Age of GDPR'. [Website], (27 June 2018), Entrepreneur. <https://www.entrepreneur.com/article/315366>.
[148] Information Commissioner's Office (ICO), 'Grants programme 2018'. [Website], (2019), Information Commissioner's Office. <https://ico.org.uk/about-the-ico/what-we-do/grants-programme-2018/>.
[149] IAPP and EY, 'IAPP-EY Annual Privacy Governance Report 2018'. [Website], (2018), IAPP. <https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf>.

consider funding mechanisms to help small businesses comply. For example, the ICO could also set up an award similar to the Regulatory Excellence Awards from the Office for Product Safety and Standards[150] which would acknowledge achievement in GDPR compliance and culminate in a showcase or conference like the ICO Data Protection Practitioners' Conference[151] where winners could share their success and challenges with others. Based on these efforts, the ICO should also learn from these companies' experiences and best practices to help guide future GDPR compliance efforts and make them more efficient and cost-effective. Initiatives like the ICO's Sandbox service, which was started 'to support organisations who are developing products and services that use personal data in innovative and safe ways', are useful ways for the ICO and industry to improve dialogue and make both sides better informed and should be explored or expanded.[152]

Second, in order for regulation to be clear, effective, and enforced, the EDPB and the national data protection agencies of the EU's member states need adequate resources and technical knowledge. Unfortunately, as already discussed, these agencies are not well-equipped to face the logistical and technical challenges of ensuring compliance with GDPR and are not always able to hold organizations accountable.[153] This is part of a broader digital skills gap in the public sector; in fact, the U.K.'s National Audit Office's 2015 survey found that in strategic, change, and technical areas, respondents identified a shortfall in skills needed.[154] Moreover, the public sector's risk-averse culture and bureaucratic processes make it challenging to put into effect new ideas and recruit and retain technological talent. Considering the complexity of technology and the fact that large tech companies like Google operate in an opaque manner via 'black box algorithms' which makes them even harder to understand,[155] regulatory agencies are at a serious disadvantage in attempting to proactively out their responsibilities, leaving companies in the driver's seat.

[150] Office for Product Safety and Standards, 'Regulatory Excellence Awards: it's time to showcase your work'. [Website], (12 February 2018), Office for Product Safety and Standards. <https://www.gov.uk/government/news/regulatory-excellence-awards-its-time-to-showcase-your-work>.
[151] Information Commissioner's Office (ICO), 'ICO welcomes data protection practitioners to 11th annual conference as privacy dominates global news agenda'. [Press release], (8 April 2018), Information Commissioner's Office. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/04/ico-welcomes-data-protection-practitioners-to-11th-annual-conference-as-privacy-dominates-global-news-agenda/>.
[152] Information Commissioner's Office (ICO), 'The Guide to the Sandbox (beta phase)'. [Website]. <https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/>
[153] Powles & Chaparro (n 68).
[154] National Audit Office, 'The digital skills gap in government'. [Website], (2015), National Audit Office. <https://www.nao.org.uk/wp-content/uploads/2015/12/The-digital-skills-gap-in-government-Survey-findings-December-2015.pdf>.
[155] Powles & Chaparro (n 68).

Consequently, it is incumbent upon the EU and member state governments to make further investments in educating civil servants on technology and address institutional factors which make hiring tech talent and innovation more difficult.[156] These difficulties can be solved in part by reforming government funding processes to incentivize change and innovation, partnering further with universities and scholars[157] on technological research and academic endeavours such as automated solutions to GDPR compliance like Oblivion,[158] investing in educational initiatives, like the U.K. Data Science Accelerator Program,[159] aimed at building technological talent in the public sector.[160] By doing so, civil servants will be in a better position to inform lawmakers about data protection issues and enforce GDPR and Article 17, substantiated by their greater understanding of technology and the digital industry.

Finally, it is important to consider citizens' understanding of data protection issues and how they can be empowered to behave more astutely online. The legal background and challenges surrounding GDPR and 'the right to erasure' are complex and given limited time and energy, it is not surprising if the average individual is less savvy than the companies attempting to access their personal data or encouraging them to share more information via social media. In fact, as the U.K.'s Office of Communications found in it is 2018 Adults' Media Use and Attitudes Report, 63% of 'social media/messaging site users…agree with the statement "I usually accept the terms and conditions without reading them on social media and messaging sites"'.[161] GDPR and its enforcement mechanisms, especially the ability for authorities to issue fines[162], are crucial in attempting to curb the power of organizations that misuse data; nevertheless, simultaneously making individuals more vigilant about how their own data is being used is also important. As

[156] Tanya Filer, *Thinking About GovTech: A Brief Guide for Policymakers* (Bennett Institute for Public Policy 2019).
[157] Information Commissioner's Office, 'Information Commissioner's Office appoints in-house expert to research and investigate the impact of Artificial Intelligence on data privacy'. [Blog]. (20 November 2018). <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/information-commissioner-s-office-appoints-in-house-expert-to-research-and-investigate-the-impact-of-artificial-intelligence-on-data-privacy/>
[158] Katherine Noyes, 'AI Can Ease GDPR Burden'. [Interview with Juan Tello], (4 June 2018), The Wall Street Journal – Deloitte. <https://deloitte.wsj.com/cmo/2018/06/04/ai-can-ease-gdpr-burden/?mod=relatedInsights>.
[159] Office for National Statistics, 'Introduction to the Data Science Accelerator programme'. [Website], (30 January 2019), Office for National Statistics. <https://www.gov.uk/government/publications/data-science-accelerator-programme/introduction-to-the-data-science-accelerator>.
[160] Filer (n 113).
[161] Office of Communications (Ofcom), 'Adults' Media Use and Attitudes Report'. [Website], (25 April 2018), Ofcom. <https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf>.
[162] Josephine Woolf, 'How Is the GDPR Doing?'. [Website], (2019), Slate. <https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html>

the Council of Europe's 2017 report on Digital Citizenship Education noted, 'privacy and security' was cited as a key component of the digital citizenship project[163]. Consequently, creating 'digital citizens', whose responsibilities include 'competent and positive engagement with digital technologies' and 'participating actively and responsibly...in communities...at all levels', is critical[164] because, as discussed, a real shift in thinking around data protection is necessary. Governments can help create digital citizens by providing easily understandable information online and through public media campaigns. Individuals should also be made aware of their rights under GDPR so that they can act under provisions like Article 17.

IV.II. LIMITATIONS AND OTHER CONSIDERATIONS

It is important to note that these recommendations are not exhaustive and will take time to develop and be implemented. They also require an investment of both time and finances to be carried out effectively. Moreover, their impact would be felt mostly in the long run and would not necessarily contribute to immediate gains in GDPR compliance and progress in carrying out the right to erasure. However, they have the potential to strengthen the impact of GDPR and Article 17.

Additionally, since the ICO and other government agencies have already taken some steps to support organizations, improve technical knowledge and skills in the civil service, and strengthen educational initiatives, it is also worth learning from these initial measures. They can provide useful insights into understanding what is and is not working in contributing to GDPR enforcement.

[163] *Ibid.*
[164] Council of Europe, 'Digital Citizenship Education: Volume 1 - Overview and new perspectives'. [Website], (2017), Council of Europe. <http://rm.coe.int/prems-187117-gbr-2511-digital-citizenship-literature-review-8432-web-1/168077bc6a>.

V. CONCLUSION

The General Data Protection Regulation is the most comprehensive set of data protection regulations ever enacted. While it is certainly not perfect and is far too ambiguous in many areas, its scope, in the E.U. and beyond, is massive. Consequently, this report has aimed at discussing some of the historical developments and challenges related to GDPR, especially Article 17, the right to erasure, with a particular focus on the U.K.

Building on a historical trajectory regarding the foundation of data protections for individuals in Europe, the right to erasure enables citizens to take more control over their digital lives. However, there are challenges in interpreting and applying GDPR including concerns related to extraterritoriality, compliance enforcement, and the balance between the individual right to privacy and the business needs of organizations. At the same time, as the world's reliance on technology increases and as more individuals' digital lives become available to businesses and organizations, it is more critical than ever for the European Data Protection Board and national data protection authorities to be able to implement data protections through GDPR effectively and equitably. Providing further support on GDPR and the ambiguities surrounding the right to erasure by helping data processors and controllers through improved helpline services and other resources, empowering the public sector, and raising awareness about data protection are all crucial endeavours in helping GDPR become more effective. As noted, the impact of these actions will not be felt immediately but over time, they can have a significant impact.

Overall, given the changing nature of the digital world, GDPR needs to be regarded as a critical first step in protecting citizens' data in the 21st century that is subject to further changes and clarifications. Considering the market power of the E.U. in addition to increasingly valid data protection concerns, it is imperative for the U.K. to ensure that its data protection regulations and enforcement power are strong and meet the needs and standards of U.K. citizens, especially with respect to Article 17.

VI. BIBLIOGRAPHY

Abdullah v. Sheridan Square Press, Inc., No. 93CIV.2515 (LLS) [SDNY 1994] 1994 WL 419847 (US).

al Khonaizi M, 'Fines under EU GDPR in Non-EU Jurisdictions: Enforceable or Mere Reputation Risk?'. [Website], (2018), Michigan Journal of International Law. <http://www.mjilonline.org/fines-under-eu-gdpr-in-non-eu-jurisdictions-enforceable-or-mere-reputation-risk/#_ftn21>

Ansip A and Jourová V, 'Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield'. [Website], (2016), European Commission. <http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm>.

Anuradha RV, 'India: What the European Union's Data Protection Rules Mean for Your Business'. [Website], (18 September 2018), Mondaq. <http://www.mondaq.com/india/x/737394/Data+Protection+Privacy/What+the+European+Unions+data+protection+rules+mean+for+your+business>.

Arthur C, 'Google Faces Deluge of Request to Wipe Details from Search Index'. [Webiste], (15 May 2014), The Guardian. <http://www.theguardian.com/technology/2014/may/15/hundreds-google-wipe-details-search-index-right-forgotten>.

'Article 8: protection of personal data' in Charter of Fundament Rights of the European Union [2012] OJ C326/02.

Astor M, 'Your Roomba may be mapping your home, collecting data that could be shared'. [Website], (25 July 2017), New York Times. <https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.>

Babel C, 'The High Costs of GDPR Compliance'. [Website], (7 November 2017), UBM. <https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263>.

Banisar D and Davies S, 'Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments', *J. Marshall J. Computer & Info. L.,* 18, 1 (1991).

Black J, 'Forms and paradoxes of principles-based regulation', *Capital Markets Law Journal,* 3/4, 425-457 (2008).

Black J, 'The rise, fall and fate of principles based regulation'. [Working Paper], (2010), London School of Economics and Political Science, Law Department. <http://eprints.lse.ac.uk/32892/1/WPS2010-17_Black.pdf>.

Boffey D, 'Dutch surgeon wins landmark "right to be forgotten" case'. [Website], (21 January 2019), The Guardian. <https://www.theguardian.com/technology/2019/jan/21/dutch-surgeon-wins-landmark-right-to-be-forgotten-case-google>.

Bowcott O, '"Right to be forgotten" could threaten global free speech, say NGOs'. [Website] (2018), The Guardian. <https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos>.

Bradford A, 'The Brussels Effect', *Northerwestern University Law Review,* 107/1, 1-68 (2012).

Burgess M, 'What is GDPR? The summary guide to GDPR compliance in the U.K.' [Website], (2019), Wired. <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>.

Butler D, 'Tomorrow's technological change is accelerating today at an unprecedented speed and could create a world we can barely begin to imagine', Nature 530, 399 (25 February 2016).

Capterra, 'GDPR Compliance Software'. [Website], (2019). <https://www.capterra.com/gdpr-compliance-software/>.

Carter E. L., 'Argentina's Right to be Forgotten', *Emory International Law Review,* 27, 23-38 (2014).

Case 101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping [2003] ECR I-12971.

Case 131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECR 317.

CEBR & SAS, 'The value of Big Data and the Internet of Things to the UK economy'. [Report], (2016), CEBR. <https://www.sas.com/content/dam/SAS/en_gb/doc/analystreport/cebr-value-of-big-data.pdf>;

Commission, 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final.

Consolidated Version of the Treaty on European Union [1992] OJ C325/5.

Couldry N and Mejias U, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject', *Television and New Media* (2 September 2018).

Council Directive (EC) 95/46 with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995].

Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, France. ETS No. 108.

Council of Europe, 'Digital Citizenship Education: Volume 1 - Overview and new perspectives' [Website], (2017), Council of Europe. <http://rm.coe.int/prems-187117-gbr-2511-digital-citizenship-literature-review-8432-web-1/168077bc6a>.

CtrlShift & U.K. Department for Digital, Culture, Media & Sport, 'Data Mobility: The personal data portability growth opportunity for the UK economy'. [Report], (2018), CtrlShift & U.K. Department for Digital, Culture, Media, & Sport. <https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf>

de Andrade N. N. G, 'Data protection, privacy and identity: Distinguishing concepts and articulating rights' in *Privacy and Identity Management for Life* (Springer 2010).

de la Torre L, 'GDPR matchup: The California Consumer Privacy Act 2018'. [Website], (31 July 2018), International Association of Privacy Professionals. <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>.

de Werra J, 'ADR in Cyberspace: The Need to Adopt Global Alternative Dispute Resolution Mechanisms for Addressing the Challenges of Massive Online Micro-Justice', *Swiss Review of International & European Law 2016,* 289-306 (2016).

Digital Millennium Copyright Act of 1998. Pub. L. 105-305. 112 Stat. 2860.

DLA Piper, 'U.K.: GDPR Brexit Flowchart'. [Website], (2018), DLA Piper. <https://blogs.dlapiper.com/privacymatters/uk-gdpr-brexit-flowchart/>.

Doubek J, 'Google Has Received 650,000 "Right to Be Forgotten" Requests Since 2014'. [Website], (2018), NPR. <https://www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014?t=1552234260819>.

Eggers W. D., Kishnani P., and Turley M, 'The Future of Regulation Principles for Regulating Emerging Technologies'. [Webiste], (2018), Deloitte Insights.

<https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation/regulating-emerging-technology.html#endnote-27>.

'Internet', Encyclopaedia Britannica. (2019) <https://www.britannica.com/technology/Internet> accessed July 2019.

EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1.

European Data Protection Board, 'About EDPB'. [Website], (2019), European Data Protection Board. <https://edpb.europa.eu/about-edpb/about-edpb_en>.

European Parliament Resolution of 12 March 2014 on the 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), COM (2012) 0011.

European Union: European Commission. (2010). Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of the Regions, COM (2010) 609 final.

European Union: European Parliament. (2010). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"). *OJ L 178*, 1–16.

European Union, 'Regulations, directives and other acts'. [Website], (2019), European Union. <https://europa.eu/european-union/eu-law/legal-acts_en>.

Filer T, 'Thinking About GovTech: A Brief Guide for Policymakers,' *Bennett Institute for Public Policy, University of Cambridge* (2018/2019).

Finck M, 'Google v CNIL: Defining the Territorial Scope of European Data Protection Law'. [Website], (16 November 2018), Oxford Business Law Blog. <https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law>.

Gabel D and Hickman T, 'Chapter 6: Data Protection Principles – Unlocking the EU General Data Protection Regulation'. [Website], (2016), White & Case. <https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection>.

GDPR Report, 'GDPR: Getting to grips with the "right to erasure" requirement'. [Website], (2018), PrivSec Report. <https://gdpr.report/news/2018/07/11/gdpr-getting-to-grips-with-the-right-to-erasure-requirement//>.

Georgiev G, 'GDPR Compliance Cost Calculator'. [Website], (2019). <https://www.gigacalculator.com/calculators/gdpr-compliance-cost-calculator.php>.

Gesetz zum Schutz vor MiBbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) of 27 January 1977, BUNDESGESETZBLATT [BGBI] 1 201 (W. Ger.) [Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act - BDSG)].

Gibbs S, 'EU to Google: expand 'right to be forgotten' to Google.com'. [Website], (27 November 2014), The Guardian. <https://www.theguardian.com/technology/2014/nov/27/eu-to-google-expand-right-to-be-forgotten-to-googlecom>.

Gibbs S, 'Google Hauled in by Europe over "Right to be Forgotten" Reaction'. [Website], (24 July 2014), The Guardian.

<https://www.theguardian.com/technology/2014/jul/24/google-hauled-in-by-europe-over-right-to-be-forgotten-reaction>.

Gooch P., Dewitt B., Luysterbourg E., Sehgal M., Sponselee A., Batch D., Frank D. P., 'A new era for privacy: GDPR six months on'. [Website], (2018), Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf>.

'Google Spain SL v. Agencia Española de Protección de Datos' (2014) 128 Harv. L. Rev. 735.

Greenleaf G, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108', *International Data Privacy Law,* 2/2, 68–92 (2012).

Guinness M, 'France maintains long tradition of data protection'. [Website], (26 January 2011), Deutsche Welle. <https://www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711>.

Hassan U, 'U.K. Tech Sector Booms to £184 Billion as "Digital Suburbs" Emerge'. [Website], (2018), Computer Business Review. <https://www.cbronline.com/news/uk-tech-sector-growing-2-6-times-faster-national-gdp>.

House of Commons Science and Technology Committee, 'Digital Skills Crisis – Second Report of Session 2016-17'. [Website], (2017), House of Commons (HC 270). <https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf>.

IAPP and EY, 'IAPP-EY Annual Privacy Governance Report 2018'. [Website], (2018). <https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf>.

Information Commissioner's Office, 'Data Protection Act 2018'. [Website], (2019), ICO. <https://ico.org.uk/for-organisations/data-protection-act-2018/>.

Information Commissioner's Office, 'Grants programme 2018'. [Website], (2019), ICO. <https://ico.org.uk/about-the-ico/what-we-do/grants-programme-2018/>.

Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)'. [Website], (2019), ICO. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>.

Information Commissioner's Office, 'The Guide to the Sandbox (beta phase). Information Commissioner's Office'. [Website], (2019), ICO. <https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/>.

Information Commissioner's Office, 'Helpline'. [Website], (2019), ICO. <https://ico.org.uk/global/contact-us/helpline/>.

Information Commissioner's Office, 'ICO welcomes data protection practitioners to 11th annual conference as privacy dominates global news agenda'. [Website], (8 April 2018), ICO. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/04/ico-welcomes-data-protection-practitioners-to-11th-annual-conference-as-privacy-dominates-global-news-agenda/>.

Information Commissioner's Office, 'Information Commissioner's Office appoints in-house expert to research and investigate the impact of Artificial Intelligence on data privacy'. [Blog], (20 November 2018), ICO. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/information-commissioner-s-office-appoints-in-house-expert-to-research-and-investigate-the-impact-of-artificial-intelligence-on-data-privacy/>.

Information Commissioner's Office, 'Information Commissioner's Office Innovation Plan – April 2017'. [Website], (April 2017), ICO. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/608843/ICO_Innovation_Plan_April_2017__1_.pdf>.

Information Commissioner's Office, 'Information Rights Strategic Plan 2017-2021'. [Website], (2017), ICO. <https://ico.org.uk/media/about-the-ico/documents/2014134/20170413icoinformationrightsstrategicplan2017to2021v10.pdf >.

Information Commissioner's Office, 'Right to erasure'. [Website], (2019), ICO. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/>.

Jourova V, 'Data Protection: Factsheet 4'. [Website], (2015), European Commission. <http://ec.europa. eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf>.

Kahn J., Bodoni S., and Nicola S, 'It'll Cost Billions for Companies to Comply With Europe's New Data Law'. [Website], (22 March 2018), Bloomberg Businessweek. <https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law>.

Knight R, 'GDPR: Small business owners still 'clueless' about data protection rules, study claims'. [Website], (12 December 2018), The Independent. <https://www.independent.co.uk/life-style/gadgets-and-tech/gdpr-data-protection-cyber-attack-security-small-businesses-aon-study-results-a8679261.html>.

Leiner B. M., Cerf V. G., Clark D. D., Kahn R. E., Kleinrock L., Lynch D. C., Postel J., Roberts L. G., and Wolff S, 'A brief history of the Internet', *ACM SIGCOMM Computer Communication Review,* 39/5, 22-31 (2009).

Loi n° 78-17 du 6 Janvier 1978 relative à L'informatique, aux Fichiers et aux Libertés.

Lomas N, 'YouTube is now taking down more videos of known extremists — in major policy change'. [Website], (2017), TechCrunch. <https://techcrunch.com/2017/11/14/in-major-policy-change-youtube-is-now-taking-down-more-videos-of-known-extremists/>.

Lomas N, 'Google Back in Court Arguing Against a Global Right to be Forgotten.'. [Website], (2018), TechCrunch. <https://techcrunch.com/2018/09/11/google-back-in-court-arguing-against-a-global-right-to-be-forgotten/>.

Magic P, 'How Small Businesses Can Survive in the Age of GDPR'. [Website], (27 June 2018), Entrepreneur. <https://www.entrepreneur.com/article/315366>.

Mantalero A, 'The E.U. Proposal for a General Data Protection Regulation and the roots of the "right to be forgotten"', *Computer Law & Security Review,* 29/3, 229-235 (2013).

Mata v Am. Life Ins. Co. [D. Del. 1991] 771 F. Supp. 1375, 1384 (US)

Matusevitch v Tenikoff [D.D.C. 1995] 877 F.Supp. 1, 2 (US)

McDermott Y, 'Conceptualising the right to data protection in an era of Big Data', *Big Data & Society,* 4/1, 1-7 (2017).

National Audit Office, 'The digital skills gap in government'. [Website], (2015), National Audit Office. <https://www.nao.org.uk/wp-content/uploads/2015/12/The-digital-skills-gap-in-government-Survey-findings-December-2015.pdf>.

NT1 and NT2 v Google LLC. [2018]. EWHC 799 (QB; EMLR 18; HRLR 13).

Noyes K, 'AI Can Ease GDPR Burden'. [Interview with Juan Tello], (4 June 2018), The Wall Street Journal – Deloitte. <https://deloitte.wsj.com/cmo/2018/06/04/ai-can-ease-gdpr-burden/?mod=relatedInsights>.

Office for National Statistics, 'Introduction to the Data Science Accelerator programme'. [Website], (30 January 2019), Office for National Statistics. <https://www.gov.uk/government/publications/data-science-accelerator-programme/introduction-to-the-data-science-accelerator>.

Office for Product Safety and Standards, 'Regulatory Excellence Awards: it's time to showcase your work'. [Website], (12 February 2018), Office for Product Safety and Standards. <https://www.gov.uk/government/news/regulatory-excellence-awards-its-time-to-showcase-your-work>.

Office of Communications (Ofcom), 'Adults' Media Use and Attitudes Report'. [Website], (25 April 2018), Ofcom. <https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf>.

Opinion of Advocate General Niilo Jääskinen, Joined Case 131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECR 317.

Payne D, 'Google, Doctors, and the "Right to be Forgotten"'. [Website], (6 January 2015), The BMJ. <https://www.bmj.com/content/bmj/350/bmj.h27.full.pdf>.

Pearson J, '"Oblivion" Is the Software That Could Automate the "Right to Be Forgotten"'. [Website], (22 June 2015), Vice. <https://motherboard.vice.com/en_us/article/4x393p/oblivion-is-the-software-that-could-automate-the-right-to-be-forgotten>.

Petzinger J, 'GDPR is the most unifying thing to happen to the E.U. in a while'. [Website], (2018), Quartz. <https://qz.com/1287872/gdpr-is-the-most-unifying-thing-to-happen-to-the-eu-in-a-while/>.

Politou E., Michota A., Alepis E., Pocs M., and Patsakis C., 'Backups and the right to be forgotten in the GDPR: An uneasy relationship', *Computer Law & Security Review,* 34/6, 1247-1257 (2018).

Powles J., and Chaparro E, 'How Google Determined Our Right to be Forgotten'. [Website], (18 February 2015), The Guardian. <https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search>.

Preliminary Ruling of 27 February 2012, *Case 131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECR 317.*

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) OJ L 119, 1-88.

Rhodes C. and Hutton G., 'The Future of the U.K. digital and tech industries'. [Debate pack], (2018), House of Commons Library, CDP 2018/0096. <http://researchbriefings.files.parliament.uk/documents/CDP-2018-0096/CDP-2018-0096.pdf>.

Satariano A, 'Google is fined $57 million under Europe's data privacy law'. [Website], (21 January 2019), New York Times. <https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html>.

Scott M and Cerulus L., 'Europe's new data protection rules export privacy standards worldwide'. [Website], (2018), Politico. <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/>.

Scott M., Cerulus L., and Overly S, 'How Silicon Valley gamed Europe's privacy rules'. [Website], (22 May 2019), Politico. <https://www.politico.com/story/2019/05/25/how-silicon-valley-gamed-the-worlds-toughest-privacy-rules-1466148>.

Simeonovski M., Bendun F., Asghar M. R., Backes M., Marnau N., and Druschel P, 'Oblivion: Mitigating Privacy Leaks by Controlling the Discoverability of Online Information' in 13th International Conference on Applied Cryptography and Network Security (ACNS 2015).

Smith B, 'Privacy Authorities Across Europe Approve Microsoft's Cloud Commitments'. [Website], (9 April 2014), Microsoft. <https://blogs.microsoft.com/eupolicy/2014/04/09/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/>.

Smith O, 'The GDPR Racket: Who's Making Money From This $9bn Business Shakedown'. [Website], (2 May 2018), Forbes. <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/>.

Solove D. J., 'A brief history of information privacy law'. [Website], (2006), Proskauer on privacy, PLI. <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2076&context=faculty_publications>.

Talend, 'The majority of businesses surveyed are failing to comply with GDPR, according to new Talend research'. [Press release], (2018), Talend. <https://www.talend.com/about-us/press-releases/the-majority-of-businesses-are-failing-to-comply-with-gdpr-according-to-new-talend-research/>.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C306/01.

U.K. Department for Digital, Culture, Media & Sport, 'Cyber Security Breaches Survey 2019'. [Website], (2019), GOV.UK. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf>.

U.S. Communications Decency Act of 1996. Pub. L. 104-104, 110 Stat. 56.

U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework Principles'. [Website], (2016). < https://www.privacyshield.gov/EU-US-Framework>.

Virginia Da Cunha v. Yahoo de Argentina S.R.L. and Google [2010] Expte. Nº 99.620/2006, Recurso Nº541.482. Juzgado Nº 75.

Wakabayashi D. and Satariano A., 'How Facebook and Google Could Benefit From the G.D.P.R., Europe's New Privacy Law'. [Website], (23 April 2018), The New York Times. <https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html>.

Warren S. D. and Brandeis L. D., 'The Right to Privacy' (1890) 4 Harv. Ll. Rev. 5, 193.

Woolf J, 'How Is the GDPR Doing?'. [Website], (2019), Slate. <https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html>.

World Bank, 'Individuals using the Internet (% of population)'. [Website], (2017), The World Bank Group. <https://data.worldbank.org/indicator/IT.NET.USER.ZS>.

Zuboff S., 'Big other: surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology,* 30/1, 75-89 (2015).

VII. ACRONYMS

AEPD: Agencia Española de Protección de Datos

ARPANET: Advanced Research Projects Agency Network

CJEU: Court of Justice of the European Union

CNIL: Commission Nationale de l'Informatique et des Libertés

DCMS: Department for Digital, Culture, Media and Sport

DPA 2018: Data Protection Act 2018

DPO: Data Protection Officer

EDPB: European Data Protection Board

EDPS: European Data Protection Supervisor

EP: European Parliament

GDPR: General Data Protection Regulation

ICO: Information Commissioner's Office

PBR: Principles-Based Regulation