Washington Journal of Law, Technology & Arts

Volume 19 | Issue 3 Article 2

6-17-2024

WHEN AI REMEMBERS TOO MUCH: REINVENTING THE RIGHT TO BE FORGOTTEN FOR THE GENERATIVE AGE

Cheng-chi Chang

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 19, ISSUE 3 — SUMMER 2024

WHEN AI REMEMBERS TOO MUCH: REINVENTING THE RIGHT TO BE FORGOTTEN FOR THE GENERATIVE AGE

Cheng-chi (Kirin) Chang[1]

ABSTRACT

The emergence of generative artificial intelligence (AI) systems poses novel challenges for the right to be forgotten. While this right gained prominence following the 2014 *Google Spain v. Gonzalez* case, generative AI's limitless memory and ability to reproduce identifiable data from fragments threaten traditional conceptions of forgetting. This Article traces the evolution of the right to be forgotten from its privacy law origins towards an independent entitlement grounded in self-determination for personal information. However, it contends the inherent limitations of using current anonymization, deletion, and geographical blocking mechanisms to prevent AI models from retaining personal data render forgetting infeasible. Moreover, the technical costs of forgetting—including tracking derivations and retraining models—could undermine enforceability. Therefore, this article advocates for a balanced legal approach that acknowledges the value of the right to forget while considering the constraints of implementing the right for generative AI. Although existing frameworks like the European Union's GDPR provide a foundation, continuous regulatory evolution through oversight bodies and industry collaboration is imperative. This article underscores how the right to be forgotten must be reconceptualized to address the reality of generative AI systems. It provides an interdisciplinary analysis of this right's limitations and proposes strategies to reconcile human dignity and autonomy with the emerging technological realities of AI. This Article's original contribution lies in its nuanced approach to integrating legal and technical dimensions to develop adaptive frameworks for the right to be forgotten in the age of generative AI.

[1] Incoming AI & The Future of Work Fellow, Emory University School of Law; Law Research Associate, Institute for Studies on AI and Law, Tsinghua University; JD, University of Florida Levin College of Law, 2024; LLM, University of Arizona James E. Rogers College of Law, 2022; LLB, National Chung Hsing University School of Law in Taiwan, 2021. I am thankful for the insightful feedback provided by Rachel Cohen, Youyang Zhong, Yilin (Jenny) Lu, Nanfeng Li, Edison Li, Shijie Xu, Yenpo Tseng, Chun-Ting Cho, Jeff Chang, Arron Fang, Ai-Jing Wu, Sabina Chen, Zih-Ting You, Li-Yin Hsiao, and Renee Wan, which enriched the content of this paper. Special thanks to Riri Wan for her thorough research support. I would like to further extend my appreciation to the editors of the *Washington Journal of Law, Technology & Arts* for their assistance in bringing this article to publication. Any errors or omissions are my sole responsibility. The views expressed in this article are solely my own and do not represent those of any affiliated institutions.

TABLE OF CONTENTS

INTRODUCTION

The growth of generative AI has reignited debates on the "right to be forgotten" in today's digital realm.[2] The right to be forgotten allows individuals to remove their personal data online, enhancing privacy. The right became notable after *Google Spain v. Gonzalez*, a 2014 European Union (EU) case. Yet, generative AI's rise challenges this right's future viability due to AI's expansive memory and data regeneration abilities.

This Article examines the legal and ethical quandaries inherent in reconciling this right and generative AI advancements. It charts the right's development from privacy protection to a distinct right of personal data control. Nevertheless, the piece argues that the AI's perpetual memory and data reconstruction might make forgetting impossible. Methods like anonymization and data removal will prove insufficient against AI's capability to recreate personal data.

Thus, this piece calls for a pragmatic legal stance that respects the right to be forgotten but acknowledges its limits. It suggests reinforcing and adapting legal structures with regulatory oversight and industry cooperation. It proposes that we need nuanced strategies that leverage generative AI for the public good while respecting personal dignity and autonomy. The Article offers a multidisciplinary review, encompassing legal, ethical, technological, and policy perspectives, of the right to be forgotten and strategies for its integration with generative AI's potential.

I. THE RIGHT TO BE FORGOTTEN

A. Concept of the Right to Be Forgotten

The concept of the right to be forgotten can be traced back to the EU's Directive on Data Protection and the free movement of such data (95/46/EC) in 1995 and the Directive on Electronic Commerce (2000/31/EC).[3] These directives formed the legal basis for search engine providers' obligation to remove links within the EU. In 2014, in *Google Spain v. Gonzales*, the European Court of Justice consolidated these directives, providing a clear legal foundation for the right to be forgotten.[4]

In the *Google Spain* case, Mr. Gonzalez requested the removal or alteration of search results related to a real estate auction that had been published in a daily newspaper by the Vanguard company.[5] He argued that the information was outdated and no longer relevant to the

---

[2] Cindy Gordon, *Google Faced With An AI Privacy Challenge: Do I Have The Right To Be Forgotten?*, FORBES (Sept. 30, 2023), https://www.forbes.com/sites/cindygordon/2023/09/30/google-faced-with-a-canadian-ai-privacy-challenge-do-i-have-the-right-to-be-forgotten/; Eduard Fosch Villaronga, Peter Kieseberg & Tiffany Li, *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, 34 COMPUTER LAW & SECURITY REVIEW 304 (2018).

[3] Council Directive No. 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(c), OJ. L 281/31 (1995); 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, 2000 O.J. L 178 1, 1.

[4] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R. 317 [hereinafter *Google Spain*].

[5] *Id.*

public or to him personally.[6] He asked Vanguard to delete or modify the publication, and Google to remove or hide the data, making it inaccessible to others.[7] The judge, citing Article 12(b) of the EU Directive 95/46/EC on Data Protection, stated that when the information processed by search engine operators is deemed inadequate, irrelevant, or excessive in relation to the objectives of data processing, both the information in question and the associated links appearing in search results are required to be removed.[8]

In 2012, the concept of the right to be forgotten was formally established in the European legal framework as a legal norm.[9] Initially, it only applied to the right to be forgotten for minors, as outlined in Article 17 of the General Data Protection Regulation (GDPR) draft.[10] However, after the official adoption of the GDPR in 2018, the right to be forgotten became applicable to all natural persons, not just minors.[11]

The term "right to be forgotten" initially referred to the idea that information, once legitimate, might lose its legitimacy over time.[12] However, the legal implications of the right to be forgotten should be analyzed from both temporal and spatial dimensions. It depends not only on the subjective judgment of the data subject but also on objective facts.[13] The right to be forgotten consists of two dimensions: the right to forget and the right to delete (including the right to object).[14] The right to forget means not keeping individuals bound to their past and providing the possibility of being "forgotten" to protect human dignity.[15] The right to delete empowers every individual to control their own information and personal data.[16] This control is supported by the concepts of the right to self-determination of personal data, the right to privacy, and the right to personal data.[17] Therefore, the legal definition of the right to be forgotten must take both the right to forget and the right to delete into account.[18] In other words, the right to be forgotten means that if the data subject does not want their personal data to be further processed or stored by a data controller and there is no legitimate reason for maintaining such data, then the data should not be accessible to the public.[19]

---

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] 2012/0011(COD): Personal Data Protection: Processing and Free Movement of data (General Data Protection Regulation), EUR. PARLIAMENT LEGIS. OBSERVATORY, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en.

[10] Proton AG, *Everything You Need to Know about the "Right to Be Forgotten,"* GDPR.EU (2018), https://gdpr.eu/right-to-be-forgotten/.

[11] Commission Regulation 2016/679, 2016 O.J. (L 119). [hereinafter *GDPR*].

[12] Jay Kaganoff, *Send the Word Over There: An Offshore Solution to the Right to Be Forgotten*, 41 NW. J. OF INT'L L. & BUS.S 245, 249–50 (2021).

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 89 (2012), https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/.

B. The Right to Be Forgotten as a Recognized Concept in Human Rights Law

The right to be forgotten has gradually evolved into a recognized concept in human rights law.[20] The right sits at the intersection of privacy, data protection, and freedom of expression, which makes it crucial to the protection of human rights. This chapter explores the evolution of the right to be forgotten from its historical roots to its status as a human right. It examines global legal frameworks that have acknowledged this right and its relationship with core human rights, particularly privacy. The chapter also analyzes the landmark *Olivier G v Le Soir* case in Belgium, instrumental in defining the right to be forgotten. It concludes by addressing the tension between this right and free speech, including the European Court of Human Rights' proposed resolutions.

1. Historical Roots and Evolution

The right to be forgotten, closely linked with the "right to erasure" as outlined in data protection laws, emerged prominently in response to the digital age's challenges.[21] This right, gaining momentum particularly after the landmark *Google Spain v. Gonzalez* case in 2014, addresses the modern dilemma where digital information is not only ubiquitous but also indelibly persistent online. This situation underscored the critical need for individuals to exert control over their personal data, a concern that was less pronounced in the pre-internet era.[22] This evolution from privacy to a recognized human rights principle can be illustrated by the European Union's General Data Protection Regulation (GDPR) in 2018, which codified the right to be forgotten as a tangible entitlement for individuals. This regulation expanded the scope beyond the traditional confines of privacy and data protection, establishing a broader human rights principle that acknowledges the nuanced implications of digital existence.[23]

While the right to be forgotten is not explicitly mentioned in most international human rights documents, it finds implicit recognition in certain provisions. The GDPR, specifically Article 17, acknowledges the right to erasure, which is deeply interconnected with human rights principles. Article 17 establishes the right of individuals to request the deletion of their personal data under specific conditions, reflecting a commitment to personal autonomy and the control of one's personal information.[24] This right is intrinsically linked to the broader human right to privacy, as encapsulated in Article 8 of the European Convention on Human Rights (ECHR), which safeguards the right to respect for private and family life. It is through this lens that the GDPR's right to erasure can be seen as a modern embodiment of the fundamental human right to privacy, ensuring that personal data protection is not just a legal obligation but a reinforcement of individuals' human dignity and autonomy in the digital age.[25] The right to privacy recognized in various international instruments, such as Article 12 of the Universal Declaration of Human

---

[20] *The Right to Be Forgotten*, *in* THE CAMBRIDGE HANDBOOK OF NEW HUMAN RIGHTS: RECOGNITION, NOVELTY, RHETORIC 285, 287–307 (Andreas von Arnauld, Kerstin von der Decken, & Mart Susi eds., 2020).

[21] Cécile De Terwangne, THE RIGHT TO BE FORGOTTEN AND THE INFORMATIONAL AUTONOMY IN THE DIGITAL ENVIRONMENT, (2013), https://publications.jrc.ec.europa.eu/repository/handle/JRC86750; ROSEN, *supra* note 19.

[22] *Id.*

[23] THE RIGHT TO BE FORGOTTEN, *supra* note 21 at 287–307.

[24] GDPR, *supra* note 11.

[25] *Id.*; Uta Kohl, *The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy*, 72 INT. COMP. LAW Q. 737 (2023).

Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), aligns with the principles underpinning the GDPR's right to erasure. These instruments collectively underscore the importance of protecting individuals from arbitrary interference with their privacy, which the GDPR operationalizes within the context of data protection. The GDPR's provisions serve to translate these international human rights norms into concrete legal mechanisms that address the complexities of personal data management in the digital era.

The right to be forgotten is inextricably linked to other fundamental human rights, with the right to privacy taking a prominent position. Article 8 of the European Convention on Human Rights (ECHR) explicitly safeguards the right to respect for private life.[26] It could be argued, particularly in light of *Olivier G v Le Soir*, that the right to be forgotten is potentially an essential aspect of the right to privacy. This perspective suggests that it enables individuals to possibly control the dissemination of their personal information and could help protect their private lives from what might be considered unwarranted intrusion.

2. Olivier G v Le Soir

The 2016 ruling of the Belgian Court of Cassation in *Olivier G v Le Soir* stands as a pivotal moment in the recognition and enforcement of the right to be forgotten within European jurisprudence.[27] Dr. Olivier G, a medical doctor, secured a seminal victory that mandated the anonymization of a 1994 online article detailing a fatal accident he caused while driving under the influence.[28] This legal triumph followed his rehabilitation and highlighted the perpetual damage to his reputation due to the article's accessibility via online search engines, overshadowing his professional and personal reform.[29]

The court's ruling in *Olivier G v Le Soir* highlighted the dynamic interplay between an individual's right to privacy and the public's right to information.[30] The decision underscored that the informational landscape had evolved significantly over the two decades since the accident, diminishing the news value of the archived article.[31] In this digital age, the ease of accessing information online perpetuates the visibility of past events, which can unjustly affect an individual's reputation long after their rehabilitation. The court acknowledged that while the freedom of expression is paramount, it is not unfettered and must be reconciled with the right to privacy.[32] Thus, the ruling recognized the importance of anonymizing the archived article in the

---

[26] European Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature Nov. 4, 1950, Eur. T.S. No. 5, 213 U.N.T.S. 221, Art. 8.

[27] Hugh Tomlinson, *Case Law, Belgium: Olivier G v Le Soir. "Right to Be Forgotten" Requires Anonymisation of Online Newspaper Archive*, INFORRM'S BLOG (2016), https://inform.org/2016/07/19/case-law-belgium-olivier-g-v-le-soir-right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive-hugh-tomlinson-qc/; Hof van Cassatie [Cass.] [Court of Cassation], 29 April 2016, AR C150052F, http://www.cass.be (Belg.) available at https://inforrm.files.wordpress.com/2016/07/ph-vog.pdf.

[28] TOMLINSON, *supra* note 27; Linda Kinstler, *Into Oblivion*, COLUMBIA JOURNALISM REVIEW (2021), https://www.cjr.org/special_report/right-to-be-forgotten.php/.

[29] TOMLINSON, *supra* note 27.

[30] *Id.* KINSTLER, *supra* note 28.

[31] TOMLINSON, *supra* note 27.

[32] *Id.*

digital sphere to protect Olivier G's rehabilitated status, illustrating a contemporary application of the right to be forgotten in balancing these competing interests.

This landmark decision carved out an approach to the right to be forgotten grounded in the essence of human dignity and reintegration into society. The Belgian courts, referencing both Article 8 of the ECHR and Article 17 of the International Covenant on Civil and Political Rights, underscored the right's intrinsic value to private life, even when pitted against the freedom of the press.[33]

As a consequence, the Court of Cassation endorsed the anonymization of the online archive, setting a precedent for the right to be forgotten to apply to digital records. The court went beyond merely preventing indexing by search engines, requiring the publisher to alter the content to protect personal rehabilitation. This case thus exemplifies the complex interplay between privacy rights and public information; a balance that continues to be recalibrated in the face of evolving technologies and enduring concerns over privacy.

C. Theoretical Foundations of the Right to Be Forgotten in Generative AI

In the previous section, I recognized the developing nature of the right to be forgotten as a human right, yet its foundation remains contested in generative AI discussions. This section explores these foundations and evaluates their importance in the era of generative AI.

The right to be forgotten deserves distinct acknowledgment in the context of generative AI. During the Web 2.0 phase, judicial rulings supported this right by implementing erasure and disengagement, helping to make it achievable. Pursuing the control over one's personal information embodies the essence of genuine human liberty, rather than a mere semblance of it.[34] However, the advancement of AI threatens this autonomy, risking the replacement of human roles and the needless revelation of personal data.[35] To mitigate these threats, we must ensure technology ethically serves the public good. Grounding the right to be forgotten in information regulation balances open access with privacy. However, without a theoretical basis, such rules could fail, resulting in erratic enforcement. Specifically, the absence of a solid theoretical foundation may lead to inconsistencies in rule application as decision-makers might interpret regulations differently without clear guidance. This could result in a lack of uniformity in enforcing the right to be forgotten where similar cases may have vastly different outcomes based on subjective interpretations of the rules. Furthermore, without a theoretical underpinning, regulations may not adequately anticipate future technological advancements, leading to gaps in protection and enforcement challenges. Thus, establishing a robust theoretical framework is crucial for ensuring that the right to be forgotten is applied consistently and evolves alongside technological progress, preventing erratic enforcement.

Exploring the foundations of the right to be forgotten necessitates a look at its ties to privacy and reputation. It expands these protections, allowing control over old personal data. In the era of Generative AI, privacy, reputation, and the right to be forgotten form a triad, each grounded in law, upholding human dignity and expanding individual liberties.

---

[33] *Id.*

[34] DE TERWANGNE, *supra* note 21.

[35] *AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data*, THE ECONOMIC TIMES, (Apr. 25, 2023), https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms.

1. Privacy Rights and the Right to Be Forgotten

In today's big data era, the clash between personal privacy and technological convenience has increased in importance.[36] Early scholars like Samuel Warren and Louis Brandeis noted the strain between technology's advantages and the inherent need for privacy.[37] Initially, privacy rights included the right to be forgotten and adapted to legal and practical shifts toward controlling personal information.[38]

The EU's right to be forgotten extends privacy to cover outdated public data. Originating in the EU's 1995 Data Protection Directive and the earlier 1981 Council of Europe Convention, this right evolved through the 2012 GDPR and European Commission clarifications in 2015. The GDPR, effective in 2016, broadened the deletion right to include voluntary and third-party shared information.[39]

Yet traditional privacy rights, which focus on personal solitude and non-disclosure outside public interest, struggle to effectively regulate obsolete public information. Thus, privacy rights and the right to be forgotten should run as distinct, parallel rights. The pre-generative AI era allowed individuals to protect their privacy through data deletion and profile adjustments.[40] But generative AI reveals a flaw in the right to be forgotten: it fails against the misuse of anonymized data.[41] Anonymized datasets in generative AI can inadvertently reveal personal details, whether incidentally through data correlation or intentionally by bad actors, thus undermining the assumption that anonymization ensures privacy.[42]

In the generative AI context, the right to be forgotten must move beyond privacy rights due to its inadequacy with anonymized data. This necessitates reevaluating its theoretical basis to match the evolving digital environment.

2. Social Identity Construction and the Right to Be Forgotten

The right to be forgotten intersects with the fundamental human right to protection against attacks on one's reputation, a concept enshrined in international law. Article 12 of The Universal Declaration of Human Rights (UDHR) explicitly safeguards an individual's honor and reputation against arbitrary interference, stating: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour

---

[36] Priyank Jain et al., *Big Data Privacy: A Technological Perspective and Review*, 3 J. BIG DATA, 25 (Nov. 26, 2016).

[37] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'").

[38] *Id.*

[39] *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR (2018), https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[40] Danielle Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 862 (2022).

[41] VILLARONGA, KIESEBERG, & LI, *supra* note 2.

[42] *Id.*; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA LAW REV. 1701, 1701 (2009) ("These scientists have demonstrated they can often 'reidentify' or 'deanonymize' individuals hidden in anonymized data with astonishing ease.").

and reputation. Everyone has the right to the protection of the law against such interference or attacks."[43] A similar protection is found in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), underscoring the global recognition of reputation as a legal right requiring defense.[44]

The right to be forgotten allows individuals to control their social identity, a need amplified by the internet's capacity to make information permanent.[45] Nicholas Goldberg, an associate editor and Op-Ed columnist for the Los Angeles Times, observes that news, which once had a transient impact, now creates enduring impressions influencing both personal and public perceptions.[46] Within this framework, the right to protection against attacks on reputation becomes particularly relevant.[47] This right is vital for individuals accused of crimes, as old or irrelevant information can obstruct their prospects and cause further harm. For instance, when information about the accused is left online, it can perpetuate the trauma for victims by continually exposing them to the details of the crime.[48] However, U.S. online platforms often fail to remove such content, citing the First Amendment. This failure to moderate can enable unfair practices like employment discrimination based solely on arrest records, which do not necessarily lead to convictions and may not reflect current legal status or rehabilitation efforts.[49]

To address egregious violations, such as revenge pornography, U.S. laws have begun to favor privacy over free speech in specific situations.[50] A core tenet of the right to be forgotten is that individuals deserve the chance to make a fresh start.[51] But not all impacts on social identity warrant the application of this right; reputation rights are more appropriate for some. This distinction is evident in the EU's divergent decisions in *Google v. CNIL*[52] and *Glawischnig-Piesczek v. Facebook Ireland*.[53] In *Google v. CNIL*, the Court of Justice of the European Union clarified that while the right to be forgotten is recognized within the EU, its application does not extend globally. The court held that search engines are not required to remove links from search

---

[43] Hof van Cassatie Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810, Art. 12 (Dec. 10, 1948).

[44] U.N. Secretary-General, International Covenant on Civil and Political Rights, U.N. Doc. S/999/14668/171 (March 23, 1976). The United States ratified the treaty Sept. 8, 1992 [hereinafter ICCPR].

[45] Yaël Ronen, *The "Right to be Forgotten" and International Crimes,* in THE RIGHT TO PRIVACY AND DATA PROTECTION IN TIMES OF ARMED CONFLICT, 286–287 (Asaf Lubin & Russell Buchan eds., 2022), https://www.repository.law.indiana.edu/facbooks/296.

[46] Nicholas Goldberg, *Column: Some Newspapers Are Deleting Old Crime Stories to Give People Fresh Starts. Is That Wise?*, L.A. TIMES (Feb. 7, 2021),

[47] RONEN, *supra* note 19 at 286–287.

[48] Zheng Xi, *Return Of A Forgotten Right: Application Of The Right To Be Forgotten In Criminal Justice*, 5 FLIS 1 (2019), https://www.heraldopenaccess.us/article_pdf/34/return-of-a-forgotten-right-application-of-the-right-to-be-forgotten-in-criminal-justice.pdf

[49] Sarah Lageson, *Criminally Bad Data: Inaccurate Criminal Records, Data Brokers, and Algorithmic Injustice*, 110–116, U. ILL. L. J, (2023), https://papers.ssrn.com/abstract=4503845.

[50] Deanna Paul, *States Are Debating Whether Revenge Porn Is Protected by the First Amendment*, WASHINGTON POST, Aug. 23, 2021, https://www.washingtonpost.com/nation/2019/05/19/is-revenge-porn-protected-by-constitution-some-states-might-say-yes/.

[51] Rachael Allen, *Who Deserves to Have Their Past Mistakes "Forgotten"?*, SLATE, Feb. 2021, https://slate.com/technology/2021/02/boston-globe-fresh-start-right-to-be-forgotten-newspapers.html.

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

[53] Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:821 (Oct. 3, 2019).

results outside of the EU, emphasizing the need to balance the right to privacy and data protection against the freedom of information and expression. This decision underscores the regional limitations of the right to be forgotten and highlights the challenges of enforcing such a right on the borderless internet. Meanwhile, the *Glawischnig-Piesczek* case suggests that defamation should be governed by reputation laws to ensure comprehensive remedies, avoiding the territorial and effectiveness constraints of the right to be forgotten.[54]

Moreover, while claims based on reputation rights alone require a high standard of proof and may not offer enough protection, the right to be forgotten responds to the digital era's broader challenges.[55] It empowers people to overcome their past amid the internet's enduring recall, which is increasingly important in the era of AI, offering a means to reconcile the imperatives of privacy and the protection of reputation in the digital age.[56]

3. Personal Information Self-Determination and the Right to Be Forgotten

Outdated information merely informs and does not necessarily affect privacy or identity. Hence, privacy rights and identity theories are inadequate for regulating the right to be forgotten. Instead, the personal information self-determination theory aptly underpins the right to be forgotten.[57] Privacy rights guard against the exposure of confidential information, while social identity concerns reputation. The right to be forgotten aims to restore the confidentiality of information that has been exposed.

Privacy and reputation rights don't encompass outdated information, which the right to be forgotten aims to rectify. As a civil and personality right, the right to be forgotten ensures data integrity, accuracy, and self-determination for individuals.[58] This right intertwines with personal information rights, forming a framework for information control.[59]

Using information self-determination as the legal basis for the right to be forgotten has distinct social benefits.[60] With blurred lines between privacy and reputation in the information age, relying on these as foundations may restrict the right's effectiveness.[61] German scholar Wilhelm Steinmüller's concept of information self-determination, which advocates for individuals to have absolute control over their private information, aligns with modern societal needs and informs current legislation like the GDPR and France's Digital Republic Act.[62]

---

[54] *Id.*

[55] Eur. Ct. H.R., *Factsheet - Protection of Reputation* (Mar. 2024), https://www.echr.coe.int/documents/d/echr/fs_reputation_eng.

[56] NICOLAS P. SUZOR, LAWLESS: THE SECRET RULES THAT GOVERN OUR DIGITAL LIVES 51–58 (2019).

[57] DE TERWANGNE, *supra* note 21, at 4–6.

[58] THE RIGHT TO BE FORGOTTEN, *supra* note 20, at 298; DE TERWANGNE, *supra* note 21, at 4–6.

[59] THE RIGHT TO BE FORGOTTEN, *supra* note 20, at 298.

[60] Florent Thouvenin, *Informational Self-Determination: A Convincing Rationale for Data Protection Law?*, 12 J. INTELL. PROP. INFO. TECH. & E-COMM.(2021), https://www.jipitec.eu/issues/jipitec-12-4-2021/5409.

[61] Jeevan Hariharan, *Damages for Reputational Harm: Can Privacy Actions Tread on Defamation's Turf?*, 13 J. MEDIA L. 186, 188 (2021).

[62] Dezheng Wang, *Research on Smart City Construction from the Perspective of Privacy Protection*, 19 US-CHINA L. REV. 312, 322 (2022); Steinmuller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider, Grundfragen des Datenschutze Gutachten im Auftrag des Bundesmnisteriums des Innern, July 1971 (BT-Drucksache VI/3826).

To conclude, the right to be forgotten should be an independent right grounded in information self-determination. While it may prompt unlimited rights claims, it must be balanced with reasonable limits, as not all claims can be absolute.

II. THE RIGHT TO BE FORGOTTEN CHALLENGES IN THE ERA OF GENERATIVE AI

The right to be forgotten is absolute in intent but limited in practice. Data's characteristics define these limits, indicating that uniform regulations may fail to adequately protect individual interests. Striking a balance between public interest and the effects of data deletion is essential.

This balancing act becomes increasingly complex in the context of generative AI. AI, in its broadest sense, refers to computer systems capable of performing tasks that typically require human intelligence.[63] This includes activities such as recognizing speech, making decisions, and translating languages.[64] Among these, generative AI, a subset of artificial intelligence, is particularly noteworthy.[65] Generative AI refers to algorithms that can generate entirely new content, including text, images, or even code, based on the data they have been trained on.[66]

Recent advancements in this field, especially with large language models (LLMs) like ChatGPT, have sparked a generative AI craze.[67] These models are trained on vast datasets and can generate highly sophisticated and human-like text, making them valuable for a myriad of applications from customer service automation to content creation.[68] However, their ability to retain and regurgitate information raises significant concerns regarding the right to be forgotten.[69]

In an age where AI might indefinitely store and replicate personal data, enforcing the right to be forgotten is a legal and technological challenge. The continuous evolution of AI algorithms and their data processing abilities, combined with privacy concerns, requires a careful analysis of data erasure's limits and possibilities. This section explores these issues and challenges.

---

[63] Darrell M. West, *What Is Artificial Intelligence?*, BROOKINGS (2018), https://www.brookings.edu/articles/what-is-artificial-intelligence/.

[64] *What Is Artificial Intelligence? Definition, Uses, and Types*, COURSERA (2023), https://www.coursera.org/articles/what-is-artificial-intelligence.

[65] Alex Friedland, *What Are Generative AI, Large Language Models, and Foundation Models?*, CENTER FOR SECURITY AND EMERGING TECHNOLOGY (May 12, 2023), https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models/.

[66] *Id.*

[67] Konstantine Buhler, *Generative AI Is Exploding. These Are The Most Important Trends You Need To Know*, FORBES (2023), https://www.forbes.com/sites/konstantinebuhler/2023/04/11/ai-50-2023-generative-ai-trends/.

[68] FRIEDLAND, *supra* note 65.

[69] Peter Grad & Tech Xplore, *Right to Be Forgotten Laws Must Extend to Generative AI, Say Researchers*, TECH XPLORE (2023), https://techxplore.com/news/2023-07-forgotten-laws-generative-ai.html.

A. AI Memory and the Right to Forgotten

The right to be forgotten is essential in digital privacy, enabling people to request the removal of personal information online.[70] Yet, AI presents new obstacles, complicating deletion due to its data processing.[71] Unlike the traditional internet, where manual removal is possible, AI's intricate operations render full data elimination nearly impossible.[72] AI's "memory," or the residual impact of previous data on subsequent outputs, further complicates total data extinction.[73]

Moreover, the trajectory of the industry suggests a growing reticence in the sharing of information, which is of particular interest when discussing AI and the right to be forgotten.[74] The trend of diminishing transparency in AI model development, as observed in the way that OpenAI and Meta AI carefully guarded details of GPT-4's architecture and Llama 2 training datasets, raises questions about the accessibility of information critical to enforcing the right to be forgotten.[75] While it may be overreaching to demand that companies disclose proprietary information, this pattern is noteworthy.[76] For instance, the Stanford Foundation Model Transparency Index, which aims to quantify the openness of AI models, rated Llama 2 at 54% and GPT-4 at 48% in transparency.[77] This lack of transparency is a trend that seems set to continue and it has significant implications for the right to be forgotten as it could hinder the ability to trace and delete personal information embedded within different AI algorithms.[78]

The proliferation of digital data, which serves as the foundation for AI, further complicates the enforcement of the right to be forgotten.[79] The increasing scale of stored digital data poses a daunting challenge for manual management.[80] As a result, individuals often have to rely on databases and algorithms to manage their personal data indirectly.[81] For example, AI systems like ChatGPT have been known to utilize personal data without explicit consent, thus

---

[70] Charlene Goldfield, *"The Right to Be Forgotten" and Its Unintended Consequences to Intelligence Gathering*, 32 FLA. J. INT'L L. 183, 185 (2022).

[71] Kate Knibbs, *Artists Allege Meta's AI Data Deletion Request Process Is a 'Fake PR Stunt,'* WIRED (Oct. 26, 2023), https://www.wired.com/story/meta-artificial-intelligence-data-deletion/.

[72] Stephen Pastis, *A.I. Trained on Private User Data Never Really "Forgets,"* FORTUNE EUR. (2023), https://fortune.com/europe/2023/08/30/researchers-impossible-remove-private-user-data-delete-trained-ai-models/.

[73] *Id.*

[74] Sebastian Raschka, *AI and Open Source in 2023*, AHEAD OF AI (Oct. 23, 2023), https://magazine.sebastianraschka.com/p/ai-and-open-source-in-2023.

[75] *Id.*

[76] *Id.*

[77] Katharine Miller, *Introducing The Foundation Model Transparency Index*, STANFORD HAI (Oct. 18, 2023), https://hai.stanford.edu/news/introducing-foundation-model-transparency-index; RASCHKA, *supra* note 74.

[78] RASCHKA, *supra* note 74.

[79] Tom Coughlin, *175 Zettabytes By 2025*, FORBES (Nov. 27, 2018), https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/.

[80] *Id.*

[81] Eric Bogert et al., *Humans Rely More on Algorithms than Social Influence as a Task Becomes More Difficult*, 11 SCI. REP. 8028 (2021).

blurring the lines between lawful and unlawful use of personal data and complicating the application of deletion rights.[82]

Instances of AI systems like ChatGPT utilizing personal data without consent, and OpenAI's mishaps leading to privacy violations, accentuate the necessity for a right to be forgotten.[83] While the issue of covert data collection and its predictive prowess, such as predicting personal attributes from social media activity, is not novel to generative AI, it nonetheless intrudes upon individual privacy and requires protective measures.[84]

In an era of pervasive interconnectivity, personal information is readily traceable and widely shared.[85] Technologies such as Software Development Kits compile data across platforms, forming enduring profiles that outlast the deletion of individual accounts.[86] This challenge intensifies when data becomes unregulated and more vulnerable to misuse even after account termination.

In light of these considerations, the right to be forgotten within the AI paradigm necessitates reevaluation. It demands a deeper understanding of AI's intrinsic "memory", the development of advanced data purging techniques, and a dynamic legal framework that keeps pace with technological innovation. This right is vital not only for safeguarding personal interests but also for ensuring the reliability of AI's predictive capabilities and fostering broad trust in our digital ecosystems.

B. The Right to be Forgotten and Public Interest

In the intricate balance between the right to be forgotten and freedom of speech, the divergent attitudes of the United States and the EU result in distinct policy outcomes. The EU's stance, as evidenced in the *Olivier G v Le Soir* case, sometimes places the right to be forgotten above freedom of speech.[87] The right to be forgotten is recognized as a fundamental human right in the *Google Spain* judgment, where it overrides not only the economic interests of data controllers, such as search engines, but also the public's right to information at times. Data controllers are defined under Directive 1995/46/EC as any "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes

---

[82] Kate O'Flaherty, *ChatGPT-4o Is Wildly Capable, But It Could Be A Privacy Nightmare*, FORBES (2024), https://www.forbes.com/sites/kateoflahertyuk/2024/05/17/chatgpt-4o-is-wildly-capable-but-it-could-be-a-privacy-nightmare/.

[83] Cat Zakrzewski, *FTC investigates OpenAI over data leak and ChatGPT's inaccuracy*, THE WASHINGTON POST, (July 13, 2023, 7:26 PM), https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/; *March 20 ChatGPT Outage: Here's What Happened*, OPENAI BLOG (Mar. 24, 2023), https://openai.com/blog/march-20-chatgpt-outage.

[84] *Facebook 'likes' predict personality*, BBC NEWS (Mar. 11, 2013), https://www.bbc.com/news/technology-21699305.

[85] Joseph Turow, *The dangers of sharing personal information on social media*, PENN TODAY (May 19, 2020), https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media.

[86] Nicole Nguyen, *A Lot Of Apps Sell Your Data. Here's What You Can Do About It.*, BUZZFEED NEWS (May 1, 2018, 8:19 AM), https://www.buzzfeednews.com/article/nicolenguyen/how-apps-take-your-data-and-sell-it-without-you-even; Jin-Hyuk Kim, Yidan Sun & Liad Wagman, *The Value of Technology Releases in the Apple iOS App Ecosystem*, 1 UNIV. OF PENNSYLVANIA (2021); Preethi Santhanam et al., *Scraping Sticky Leftovers: App User Information Left on Servers After Account Deletion*, 2022 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP) 2145 (2022), https://www.computer.org/csdl/proceedings-article/sp/2022/131600a330/1FlQH93iQJa.

[87] TOMLINSON, *supra* note 28; KINSTLER, *supra* note 28.

and means of the processing of personal data." Consequently, search engines are considered data controllers as they determine how personal data is processed through the management of online search results. They are responsible for considering requests for erasure of data, weighing these requests against public interest.[88] Data processors, in contrast, handle personal data on behalf of a data controller and act according to their directives.[89]

In contrast, the U.S. regards freedom of speech and the press as fundamental, with privacy rights, including the right to be forgotten, stemming from judicial readings of the Constitution rather than direct statements. The pivotal case of *Griswold v. Connecticut* identified privacy rights within the Fourteenth Amendment, though these rights are not listed, unlike the explicit safeguards for speech and press in the First Amendment.[90] *Cox Broadcasting v. Cohn* illustrates this principle, confirming that spreading legally acquired, accurate information about significant public issues is protected speech.[91]

The legal split highlights that the right to be forgotten, constrained by public interest, is not absolute. The capacity of some generative AIs, such as DALL-E, to create non-consensual deepfakes carries a significant risk to personal reputation and autonomy.[92] AI presents new challenges in reconciling the right to be forgotten with public interest, potentially maintaining a person's image in the public sphere beyond their right to data erasure.[93]

The EU's incorporation of the right to be forgotten within the GDPR aims to protect individuals from AI data handlers' monopolistic behaviors.[94] However, as AI evolves, debates around data nationalism—the practice of countries asserting control over data generated within their borders—and unrestricted data flow may intensify, especially regarding international data protection laws.[95]

The U.S. opposes the EU's push for global enforcement of the right to be forgotten due to digital sovereignty concerns, a stance some critics as "digital colonialism."[96] This affects search engines, which struggle with the complexities of international data retrieval and the right to be forgotten.[97]

C. The Cost of Forgetting and the Dilemma of Forgetting

The debate over the right to be forgotten and AI hinges on whether AI embodies a concept of memory akin to human understanding. Scientists largely agree that data retention

---

[88] TOMLINSON, *supra* note 28.

[89] *Id.*

[90] Griswold v. Conn., 381 U.S. 479 (1965).

[91] Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975).

[92] Mack DeGeurin, *DALL-E Users Can Now Upload and Edit Real Human Faces. What Could Possibly Go Wrong?*, GIZMODO (Sept. 20, 2022), https://gizmodo.com/dall-e-ai-openai-deep-fakes-image-generators-1849557604.

[93] Avi Gesser et al., *Debevoise Discusses Malicious Corporate Deepfakes*, CLS BLUE SKY BLOG (Feb. 1, 2023), https://clsbluesky.law.columbia.edu/2023/02/01/debevoise-discusses-malicious-corporate-deepfakes/.

[94] Dirk Bergemann et al., *Market Design for Personal Data*, 40 YALE J. ON REGUL. 1056, 1104–05 (2023), https://openyls.law.yale.edu/handle/20.500.13051/18331.

[95] Anupam Chander & Uyên Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015).

[96] Gordon LaForge & Patricia Gruver, *Governing the Digital Future*, NEW AMERICA (Oct. 2023), http://newamerica.org/planetary-politics/reports/governing-the-digital-future/.

[97] *Id.*

equates to memory.[98] This complexity becomes apparent with expansive AI models like GPT-4 and DALL-E, trained on diverse, massive datasets.[99] Understanding the training process can shed light on this issue. During training, AI models ingest vast amounts of data, learning patterns and relationships within the dataset. This process embeds information into the model's parameters, enabling it to generate responses or predictions based on the learned data. However, once integrated, these models inherently lack the function to "forget" or discard specific data, as their architecture is designed to utilize all available information for optimal performance. This absence of a forgetting mechanism presents significant challenges for the implementation of the right to be forgotten in the context of AI.[100]

The principle of the right to be forgotten, while applicable to personal data, encounters significant hurdles when applied to AI.[101] For instance, an AI like DALL-E is trained on countless images and concepts to generate new visuals and cannot easily isolate and eliminate specific data points post-training.[102] The scale of the datasets used to train such models—which can span billions of parameters—and the interconnectedness of this information within the neural network make selective forgetting a formidable technical challenge.[103]

The GDPR's stipulation that forgotten information should not be accessible does not ensure that data is deleted from the AI system; removal efforts may merely alter the form that the data exists in.[104] In AI models, fragments of "forgotten" data can still influence outcomes, as the learning is an integral part of the model's "memory."[105] Hence, a true "right to be forgotten" within AI systems currently seems more conceptual than practical.[106] To execute a complete "forgetting," significant technical advancements are required; not just policy changes.[107] For large-scale AI models, this could entail the enormous task of retraining with revised datasets—a process both resource-intensive and potentially unfeasible for continuous requests.[108]

---

[98] Gregorio Zlotnik & Aaron Vansintjan, *Memory: An Extended Definition*, 10 FRONT. PSYCH. (2019), https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2019.02523/full (last visited May 23, 2024) ("'memory' now is used to refer to storage of information in general, including in DNA, digital information storage, and neuro-chemical processes.").

[99] Melissa Heikkilä, *OpenAI's Hunger for Data Is Coming Back to Bite It*, MIT TECH. REV. (Apr. 19, 2023), https://www.technologyreview.com/2023/04/19/1071789/openais-hunger-for-data-is-coming-back-to-bite-it/; Ryan O'Connor, *How DALL-E 2 Actually Works*, ASSEMBLYAI (Sept. 29, 2023), https://www.assemblyai.com/blog/how-dall-e-2-actually-works/.

[100] HEIKKILÄ, *supra* note 99; Rachel Layne, *How to Make AI "Forget" All the Private Data It Shouldn't Have*, HBS WORKING KNOWLEDGE (2024), http://hbswk.hbs.edu/item/qa-seth-neel-on-machine-unlearning-and-the-right-to-be-forgotten (last visited May 23, 2024).

[101] *Id.*

[102] O'CONNOR, *supra* note 99; KNIBBS, *supra* note 71; HEIKKILÄ, *supra* note 99.

[103] KNIBBS, *supra* note 71; Kali Hays, *OpenAI Offers a Way for Creators to Opt out of AI Training Data. It's so Onerous That One Artist Called It "Enraging.,"* BUSINESS INSIDER (Sep. 29, 2023), https://www.businessinsider.com/openai-dalle-opt-out-process-artists-enraging-2023-9.

[104] Matt Burgess, *How To Delete Your Data From ChatGPT*, WIRED (May 9, 2023), https://www.wired.com/story/how-to-delete-your-data-from-chatgpt/.

[105] PASTIS, *supra* note 72.

[106] *Id.*

[107] *Id.*

[108] *Id.*

Furthermore, the right to be forgotten in the context of AI is complicated by the fact that these systems do not forget their training.[109] Instead, the data becomes part of a complex web of learned patterns and predictions, making the removal of specific data points akin to altering memories embedded within a human brain.[110]

Practically, enforcing the right to be forgotten requires a multifaceted approach, considering not just the costs but also the technical feasibility.[111] As the case of Google's application process for the right to be forgotten demonstrates, the evaluation and enforcement process is intricate and labor-intensive.[112] With AI systems, this process would be even more complex, necessitating constant monitoring and potentially retraining models, which is not always practical due to its cost.[113]

In conclusion, while the right to be forgotten is a crucial aspect of privacy and data protection laws, its implementation in the realm of AI, particularly with generative models like GPT-4 and DALL-E, presents unprecedented technical challenges. These challenges require a re-examination of what "forgetting" means in the context of machine learning and how it can be practically achieved, if at all. Without addressing these technical challenges, the right to be forgotten may remain a theoretical construct rather than an enforceable right when it comes to AI.

III. FORGING A STRONG RIGHT TO BE FORGOTTEN FRAMEWORK IN THE AI ERA

A. Safeguarding Information Rights in AI's Era of Forgotten Data

Enhanced computing power and data collection have propelled AI advancements. Notably, Alpha Go's triumph over Go champion Lee Sedol highlighted the potency of AI algorithms, which now permeate law, healthcare, education, and transportation sectors, performing cognitive functions like humans.[114] Further AI applications range from self-driving cars to robotic surgery, signaling a harmonious AI-industrial synergy.[115]

The legal acknowledgment of the right to be forgotten can mitigate AI-related data risks, such as unauthorized data collection and leakage. Unlike simpler internet products, AI's

---

[109] Miguel Luengo-Oroz, *We Forgot To Give Neural Networks The Ability To Forget*, FORBES (Jan. 25, 2023, 11:30 AM), https://www.forbes.com/sites/ashoka/2023/01/25/we-forgot-to-give-neural-networks-the-ability-to-forget/.

[110] *Id.*

[111] Peter Druschel, Michael Backes, & Rodica Tirtea, *The Right to Be Forgotten - between Expectations and Practice*, ENISA, 8–13 (2012), https://www.enisa.europa.eu/publications/the-right-to-be-forgotten.

[112] *Right to Be Forgotten Overview*, GOOGLE, https://support.google.com/legal/answer/10769224?hl=en&sjid=18412393822176023237-NA (last visited May, 22, 2024).

[113] Samuel Greengard, *Can AI Learn to Forget?*, 65 COMMUN. ACM 9 (2022), https://dl.acm.org/doi/pdf/10.1145/3516514.

[114] Steven Borowiec, *AlphaGo Seals 4-1 Victory over Go Grandmaster Lee Sedol*, THE GUARDIAN (Mar. 15, 2016, https://www.theguardian.com/technology/2016/mar/15/googles-alphago-seals-4-1-victory-over-grandmaster-lee-sedol.

[115] Andrew A. Gumbs et al., *Artificial Intelligence Surgery: How Do We Get to Autonomous Actions in Surgery?*, 21 SENSORS (BASEL) 5526 (2021).

complexity defies easy prediction, necessitating dedicated regulatory oversight.[116] The right to be forgotten, paired with the right to deletion, empowers individuals to manage their personal data, addressing the imbalance favoring information controllers.

To address the complex and enduring risks posed by AI, particularly in light of current regulatory deficits, a broadened right to be forgotten is imperative. This right should be comprehensive, covering the entire data lifecycle, which includes collection, storage, processing, and deletion phases. Each phase presents unique challenges and characteristics; therefore, adaptations of the right to be forgotten must take into account the specific requirements and contexts of these distinct phases to ensure effective implementation. AI poses complex, enduring risks that are amplified by regulatory deficits. Broadening the right to be forgotten is imperative for moving toward a solution.[117] This expansion should encompass the entire data lifecycle, adapting to the distinct characteristics and challenges presented at each stage of data management.[118]

B. Tailored Legal Protection for Diverse Right-Holders

Due to the inherently personal nature of the right to be forgotten, the right pertains only to individuals and excludes corporations or organizations.[119] It safeguards personal data security but does not apply to legal entities, which cannot experience psychological damage from personal data breaches.[120] Furthermore, extending the right to be forgotten to corporations could lead to abuse of the right and compromise personal data protection aims.[121]

Natural persons are all entitled to the right to be forgotten, yet claims vary with the claimant's status. This Article proposes a tiered protection system, offering nuanced protection reflecting the individual's legal capacity and identity.

Minors, the mentally ill, and those with limited civil capacity warrant heightened protection due to their vulnerability. For instance, California's "Online Eraser Law" provides a model for safeguarding minors by mandating clear deletion procedures without scrutinizing their deletion requests.[122] Likewise, the mentally ill, being equally vulnerable, should be protected in a similar manner with guardians facilitating deletion requests when necessary.

Public figures and officials should have a more limited right to be forgotten. While lacking a precise legal definition, public figures include celebrities and individuals with public

---

[116] Ted Lieu, *Opinion, I'm a Congressman Who Codes. A.I. Freaks Me Out.*, THE N.Y. TIMES (Jan. 23, 2023), https://www.nytimes.com/2023/01/23/opinion/ted-lieu-ai-chatgpt-congress.html.

[117] Kevin Roose, *A.I. Poses 'Risk of Extinction,' Industry Leaders Warn*, THE N.Y, TIMES (May 30, 2023), https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html.

[118] John Frank Weaver, *Artificial Intelligence and Governing the Life Cycle of Personal Data*, 24 RICHMOND J. LAW TECHNOL. 1, 11–12 (2017) ("personal data governance should focus on the life cycle of personal data and address each stage individually").

[119] European Commission, *Do the Data Protection Rules Apply to Data about a Company?*, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en.

[120] B. van der Sloot, *Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-Tiered System*, 31 COMPUTER LAW & SECURITY REVIEW 26 (2015).

[121] EUROPEAN COMMISSION, *supra* note 119.

[122] Rahul Kapoor, W. Reece Hirsch, & Shokoh H. Yaghoubi, *Get to Know California's 'Online Eraser' Law*, THE NATIONAL LAW REVIEW (2016), https://www.natlawreview.com/article/get-to-know-california-s-online-eraser-law.

influence.[123] Extensive rights for public figures could lead to misuse, allowing them to use the right to escape public accountability. Yet, they deserve protection against discrimination and excessive personal data exploitation due to their visibility, particularly via AI. Public officials, due to their role, should be accountable to public scrutiny, but this consideration needs to be balanced with the privacy rights still enjoyed by these individuals.

The right to be forgotten for criminals remains contentious.[124] A restrictive approach is advocated for general offenders, considering the diminishing relevance of criminal records over time.[125] Offenders need this right to reintegrate into society post-punishment. Nonetheless, differentiation is crucial based on the crime's nature and the offender's profession. In particular, certain crimes by educators or public servants should exempt them from this right.

C. Harmonizing Legal and Technological Frontiers in AI Governance

Discourse surrounding AI governance often focuses on how regulation might impede technological progress, particularly within the sphere of AI.[126] The "Ten Principles for Regulation That Does Not Harm AI Innovation" report by The Information Technology and Innovation Foundation provides a blueprint for a regulatory approach that both nurtures innovation and addresses potential concerns.[127] These principles advocate for regulations that are performance-based rather than prescriptive, tailored to specific sectors as opposed to blanket policies across technologies, and adaptable enough to incorporate future technological breakthroughs.[128] The principles underscore the necessity of regulatory efficiency, thorough cost-benefit analyses, impartiality towards firms, and the critical role of technical expertise in policy-making.[129]

This framework exemplifies the intricate balance between law and technology, where each must be responsive to the other's evolution. AI systems, embodying the values and intentions of their designers, necessitate the integration of legal principles to ensure they both benefit the public and conform to societal expectations.[130] A vital aspect of this interplay is

---

[123] Shlomit Yanisky-Ravid & Ben Zion Lahav, *Public Interest vs. Private Lives--Affording Public Figures Privacy in the Digital Era: The Three Principle Filtering Model*, 19 UNIV. PA. J. CONST. LAW 975 (2017) ("The U.S. courts have used a great many examples to define the category of "public figure, including, but not limited to: [1] celebrities [i.e., people from the entertainment sector]; [2] those holding or formerly holding public office, including politicians and other elected officials; [3] criminals; [4] inventors, researchers, and academics [5] war heroes; [6] figures from the news; and [7] unwilling or unexpected public figures [e.g., someone who was at the scene of a crime or in a demonstration], amongst others.").

[124] XI, *supra* note 48.

[125] *Id.*

[126] Tom Wheeler, *The Three Challenges of AI Regulation*, BROOKINGS (June 15, 2023), https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/.

[127] Daniel Castro, *Ten Principles for Regulation That Does Not Harm AI Innovation* CTR. FOR DATA INNOVATION 1 (Feb. 8, 2023), https://itif.org/publications/2023/02/08/ten-principles-for-regulation-that-does-not-harm-ai-innovation/.

[128] *Id.*

[129] *Id.*

[130] LEGALTECH NEWS, *Tracking Generative AI: How Evolving AI Models Are Impacting Legal*, LAW.COM (Feb. 29, 2024), https:/www.law.com/legaltechnews/2023/11/17/tracking-generative-ai-how-evolving-ai-models-are-impacting-legal.

finding an equilibrium between encouraging technological innovation and protecting individual rights, including privacy. The European GDPR exemplifies a forward-thinking stance on data management, particularly with its provision for the right to be forgotten, highlighting a shift towards preemptive risk management in AI regulation.

To fortify the legal framework around AI, it is crucial to advocate for a robust push towards industry self-regulation, complemented by governmental oversight.[131] This tandem approach leverages the industry's nimbleness and technical acumen with the democratic legitimacy and broader perspective of public regulation.[132] For example, the European Union's AI Act and other national efforts demonstrate proactive legislative endeavors, while the tech industry's voluntary adoption of the OECD's AI Principles showcases the potential for self-regulation to set benchmarks for responsible AI use.[133] This collaborative dynamic can result in potent and adaptable regulations that keep pace with AI's swift evolution, ensuring that the right to be forgotten remains a viable concept in the generative AI era.

The US should build upon the GDPR model by adopting strategies that encourage industry self-regulation while ensuring AI systems are congruent with societal norms and individual liberties. Such a comprehensive strategy, grounded in the principles from the Information Technology and Innovation Foundation report, could establish a comprehensive framework for the right to be forgotten in the age of AI.[134] This approach would allow for technological progress while maintaining the essential human right to privacy and the ability to control one's personal information. Moreover, the agility of self-regulation can be instrumental in addressing the unique challenges posed by generative AI. Initiatives like Meta's Oversight Board, which offers rapid and discretionary decisions on content moderation, exemplify the potential for self-regulation to operate beyond the constraints of geography and uniform legal systems.[135] However, self-regulation must be viewed critically, ensuring that it serves the public interest and not just corporate goals. Transparency and accountability are paramount to gain public trust and to ensure that self-regulatory bodies are not merely extensions of their parent corporations.[136] A balanced approach to self-regulation in AI, therefore, should prioritize citizen outcomes, safeguarding transparency, and upholding ethical standards while fostering innovation.[137]

Geopolitical considerations influence AI's regulatory landscape, particularly in the context of the global technological race.[138] It is essential to address the misconception that U.S.

---

131 Thomas Hemphill & Phil Longstreet, *How Private Governance Mitigates AI Risk*, THE CTR. FOR GROWTH AND OPPORTUNITY (Sept. 2023), https://www.thecgo.org/research/how-private-governance-mitigates-ai-risk/.

132 Alex Engler, *The EU and U.S. Diverge on AI Regulation: A Transatlantic Comparison and Steps to Alignment*, THE BROOKINGS INST. (Apr. 25, 2023), https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/.

133 Alyssa Wong, *Regulatory Gaps and Democratic Oversight: On AI and Self-Regulation*, SCHWARTZ REISMAN INSTITUTE (2023), https://srinstitute.utoronto.ca/news/tech-self-regulation-democratic-oversight (last visited May 23, 2024).

134 CASTRO, *supra* note 127.

135 WONG, *supra* note 133.

136 Adonis Hoffman, *Why Self-Regulation Is Best for Artificial Intelligence*, THE HILL (Nov. 8, 2023), https://thehill.com/opinion/4300288-why-self-regulation-is-best-for-artificial-intelligence/ (last visited May 23, 2024).

137 *Id.*

138 Helen Toner, Jenny Xiao, & Jeffrey Ding, *The Illusion of China's AI Prowess*, FOREIGN AFFAIRS, (Jun. 2, 2023), https://www.foreignaffairs.com/china/illusion-chinas-ai-prowess-regulation.

regulations, including the right to be forgotten, could hinder AI progress and inadvertently advantage non-U.S. entities, notably Chinese companies. This concern stems from the perception that stringent U.S. regulations could stifle innovation, whereas Chinese companies might operate more freely. However, this view overlooks the significant regulatory and technological challenges faced by Chinese AI developers, including their reliance on U.S. technology.[139] The reality is that both U.S. and Chinese AI sectors operate under substantial regulatory scrutiny, and the implementation of the right to be forgotten in the U.S. would not necessarily confer a competitive advantage to Chinese companies.[140] Instead, by reinforcing the right to be forgotten, the U.S. would emphasize the importance of privacy and autonomy in AI development, aligning technological advancement with democratic values without necessarily impeding its own AI sector's competitiveness.[141] This approach counters the narrative of China's unassailable lead in AI by demonstrating a commitment to ethical AI development that respects individual rights.[142] Therefore, incorporating the right to be forgotten into AI governance is a strategic move to balance innovation with ethical considerations, reflecting a broader commitment to privacy and autonomy without undermining the perception of American AI capabilities. OpenAI's recent shift towards capitalist priorities and away from conservative nonprofit governance exemplifies the tech sector's broader preference for profit over safety.[143] This new direction, steered by business leaders, emphasizes the prioritization of economic returns in AI development.[144]

OpenAI's shift in priorities underscores the need for balanced AI regulation that includes considerations such as the right to be forgotten. AI's increasing prominence, evidenced by tools like ChatGPT, demands regulations that protect individual rights alongside innovation. The right to be forgotten is key among these regulations. As AI entwines with daily life, its misuse could damage individual privacy rights. OpenAI's shift mirrors the industry's wider move but also highlights the chance to embed privacy and autonomy rights into corporate practices.[145] The growing debate on this right within AI circles isn't just about control—it's about instilling regulations based on values that protect against AI's possible overreach.[146]

---

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] Kevin Roose, *A.I. Belongs to the Capitalists Now*, THE N.Y. TIMES, (Nov. 22, 2023), https://www.nytimes.com/2023/11/22/technology/openai-board-capitalists.html.

[144] *Id.*

[145] *Id.*

[146] United Nations, *Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet*, OHCHR (2021), https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet ("AI systems rely on large data sets, with information about individuals collected, shared, merged and analysed in multiple and often opaque ways. The data used to inform and guide AI systems can be faulty, discriminatory, out of date or irrelevant. Long-term storage of data also poses particular risks, as data could in the future be exploited in as yet unknown ways."); Matthew Hutson, *Rules to Keep AI in Check: Nations Carve Different Paths for Tech Regulation*, 620 NATURE 260 (2023).

D. Balancing Rights and Innovation in Algorithm Oversight

International efforts to regulate generative AI, namely ChatGPT, are instructive to agencies seeking to strike a balance between protecting rights and promoting innovation. The enforcement action by the Italian Garante, Italy's Data Protection Authority, against ChatGPT exemplifies the urgent need for effective regulatory frameworks consistent with the EU's GDPR.[147]

The Garante's intervention in Italy was a significant regulatory action addressing OpenAI's compliance with the GDPR. This intervention was not an isolated event but part of a broader European effort to enforce data protection laws amidst the rise of generative AI technologies like ChatGPT. The Garante identified specific concerns regarding transparency in data processing, the legal basis for data collection, the accuracy of generated information, and safeguards for minors.[148] These concerns were based on potential violations of Articles 5, 6, 8, 13, and 25 of the GDPR, which collectively mandate the protection of personal data, the lawfulness of processing, and the conditions for obtaining consent from children. The Italian authority's decision to require OpenAI to implement corrective measures, including enhancing transparency and establishing age verification systems, reflects the EU's commitment to upholding privacy rights and the integrity of personal data.[149]

To address these violations, the Italian Garante set forth a series of corrective measures for OpenAI.[150] The Garante required OpenAI to enhance transparency by clarifying data processing methods and users' rights, ensure data processing had a legitimate legal basis, and provide mechanisms for data subjects to exercise their rights, such as correcting or deleting inaccurate data.[151] Furthermore, the Garante required OpenAI to comply with the GDPR's child protection requirements by implementing age verification systems for minors under the age of 13.[152]

The developments in Italy underscore the necessity for a dedicated Algorithm Committee to ensure AI oversight.[153] An Algorithm Committee would serve as a centralized body responsible for the review and supervision of AI algorithms, ensuring compliance with regulatory standards such as the GDPR. It would also provide a mechanism for addressing the concerns raised by the Garante, such as improving transparency in data processing methods, verifying the legal basis for data collection, and implementing safeguards for the accuracy of information and child protection. This committee's role would be crucial in maintaining a

---

[147] Frances D'Emilio & Matt O'Brien, *Italy Temporarily Blocks ChatGPT Over Privacy Concerns*, AP NEWS (2023), https://apnews.com/article/chatgpt-ai-data-privacy-italy-66634e4d9ade3c0eb63edab62915066f.

[148] *Provvedimento del 30 marzo 2023 [9870832]*, ITALIAN DATA PROT. AUTH. (2023), https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9870832; D'EMILIO & O'BRIEN, *supra* note 147.

[149] *Provvedimento del 30 marzo 2023 [9870832]*, ITALIAN DATA PROT. AUTH. (2023), https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9870832; Kevin Roose, *A.I. Belongs to the Capitalists Now*, THE N.Y. TIMES, (Nov. 22, 2023), https://www.nytimes.com/2023/11/22/technology/openai-board-capitalists.html; D'EMILIO & O'BRIEN, *supra* note 147.

[150] D'EMILIO & O'BRIEN, *supra* note 147.

[151] ITALIAN DATA PROT. AUTH., *supra* note 148.

[152] *Id.*

[153] *Human Rights & Technology Issues Paper UTS Submission*, UNIV. OF TECH. SYDNEY, 59–61 (2018), https://www.uts.edu.au/sites/default/files/2018-12/Human%20Rights%20%26%20Technology%20Issues%20Paper_UTS%20submission.pdf.

balance between protecting individual rights and fostering innovation, as it would provide a structured approach to algorithmic accountability and compliance with privacy laws.[154]

The right to understand algorithmic decisions is pivotal to this new oversight approach. Given the intricacy of AI systems like ChatGPT, only a centralized authority can provide transparent communication about their workings.[155] Additionally, supervision should be proactive, integrating risk management throughout the data lifecycle. The committee would also handle data deletion rejections and algorithm-related corporate disputes, thus promoting legal precision and personal privacy.

Inspired by France's 'Information Technology and Freedom Law' and the Commission Nationale de l'Informatique et des Libertés (CNIL), the U.S. could benefit from a similar governance structure through the establishment of the National Artificial Intelligence Advisory Committee (NAIAC). The French model offers a comprehensive approach to data protection, with the CNIL handling a significant number of cases involving advice requests, complaints, and opinions on personal data processing. The French system emphasizes the importance of managing sensitive data, such as health information, through the implementation of secure intranet networks and smart card technology. Moreover, the CNIL's proactive stance on issues like behavioral mega-databases and ambiguous data collection practices showcases a commitment to clear and honest communication of data usage to individuals. Adopting a model akin to France's would enable the U.S. to foster robust protections for individual rights, particularly in the context of AI's rapid development. The NAIAC could serve as a platform for ensuring that AI advancements align with legal standards, promoting transparency and accountability in data processing. By incorporating the French approach, the U.S. stands to gain from a regulatory framework that not only safeguards privacy but also facilitates the responsible and ethical use of AI technologies.[156]

The Garante's proactive stance and the subsequent resumption of ChatGPT's operations in Italy following compliance adjustments set a precedent for international AI governance.[157] It exemplifies the potential for a cooperative model where AI developers, users, and regulatory bodies work together to achieve a balance between protecting personal rights and fostering technological advancement. The authority highlighted the need for clear mechanisms that enable individuals to request the deletion or correction of their personal data, in compliance with the

---

[154] *Id.*

[155] Comer & Raskin Introduce the Federal AI Governance and Transparency Act, UNITED STATES HOUSE COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY (2024), https://oversight.house.gov/release/comer-raskin-introduce-the-federal-ai-governance-and-transparency-act/ (The bipartisan Federal AI Governance and Transparency Act in the U.S. highlights the importance of having a structured oversight framework for AI systems to ensure compliance with privacy laws and civil rights.); Varun Aggarwal, *Senate Leaders Propose New Bipartisan Framework for AI Regulation*, HARVARD JOURNAL OF LAW & TECHNOLOGY (2023), https://jolt.law.harvard.edu/digest/senate-leaders-propose-new-bipartisan-framework-for-ai-regulation (The recent bipartisan framework for AI regulation proposed by U.S. Senate leaders also stresses the creation of an independent licensing and oversight body. This body would be responsible for ensuring legal accountability for harms caused by AI and promoting transparency through mandatory audits and public disclosure of AI system details, including training data and safety measures).

[156] *Second Annual Report. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. Adopted 30 November 1998*, EUR. UNION, 12–13 (1998), http://aei.pitt.edu/42294/.

[157] Supantha Mukherjee & Giselda Vagnoni, *Italy restores ChatGPT after OpenAI responds to regulator*, REUTERS (Apr. 28, 2023, 2:01 PM), https://www.reuters.com/technology/chatgpt-is-available-again-users-italy-spokesperson-says-2023-04-28/.

GDPR. This included ensuring that data processing by AI systems has a lawful basis, that there is transparency in how personal data is used, and that individuals, particularly minors, are provided with adequate protections. The Garante's focus on these aspects emphasizes the importance of the right to be forgotten as AI systems become more prevalent, setting a precedent for how such cases may be handled in the future and reinforcing the need for AI developers to incorporate the right to be forgotten considerations into their operations.

E. Balancing the Right to be Forgotten with the Advancement of AI

In the evolving AI landscape, balancing privacy and progress is essential. The EU's GDPR enshrines the right to be forgotten, allowing individuals to control their data and request deletion of harmful or unnecessary information. Its principles—privacy by design, data minimization, clear purpose specification, and restricted retention—ensure enforcement of these rights across the EU.

In light of this, researchers from Microsoft, Ronen Eldan and Mark Russinovich, have contributed significant research in AI data management.[158] Their work, "Who's Harry Potter? Approximate Unlearning in LLMs," presents a method for LLMs to selectively forget copyrighted content without requiring a complete model retrain.[159] This approach is particularly relevant for legal compliance, offering a practical implementation of the right to be forgotten within AI.

Eldan and Russinovich propose a method that involves the creation of a "forgetting dataset" to refine the base model, ensuring the model forgets specific copyrighted content while retaining its broader linguistic capabilities.[160] This technique maintains the model's performance on standard datasets while preventing it from generating the forgotten content, demonstrating a promising step towards reconciling the right to be forgotten with technological development.[161]

Furthermore, transparency and explainability in AI are crucial for user trust. Explainability, or interpretability, refers to the degree to which the internal mechanisms of an AI system can be understood by humans. This necessitates clear operations of algorithms to facilitate informed consent, allowing users to comprehend how decisions are made.[162] Transparency, closely related to explainability, enhances users' ability to challenge or rectify automated decisions and effectively mitigates algorithmic bias.[163]

This synergy between legal principles and technological innovations underscores the importance of privacy in the digital age, suggesting a path forward where individuals' dignity and equality are preserved alongside the growth of AI, ultimately supporting a robust digital ecosystem where innovation thrives within the bounds of ethical and legal standards.

---

[158] Ronen Eldan & Mark Russinovich, *Who's Harry Potter? Approximate Unlearning in LLMs*, ARXIV (Oct. 4, 2023), http://arxiv.org/abs/2310.02238.
[159] *Id.*
[160] *Id.*
[161] *Id.*
[162] Donghee Shin, *User Perceptions of Algorithmic Decisions in the Personalized AI System: Perceptual Evaluation of Fairness, Accountability, Transparency, and Explainability*, 64 J. OF BROADCASTING & ELECTRONIC MEDIA 541 (2020).
[163] *Id.*

CONCLUSION

The right to be forgotten represents a complex intersection of law, technology, and ethics. As this article has explored, the emergence of generative AI adds new dimensions that challenge traditional conceptions of privacy, data protection, and the feasibility of forgetting. While existing laws like the GDPR provide an initial framework, effectively safeguarding the right to be forgotten in the AI era necessitates a comprehensive and nuanced approach.

Key conclusions can be drawn from this analysis. First, the right to be forgotten must be established as an independent right grounded in personal information self-determination, beyond just privacy and reputational rights. This empowers individuals to control their data within AI systems. Second, the inherent limitations of AI technology in "forgetting" data must be acknowledged in efforts to balance individual rights with technical constraints and public interests. Regulatory creativity is needed to address the traceability of anonymized data. Third, continuous evolution of legal frameworks is imperative through oversight bodies, industry collaboration, and international cooperation. As this article has contended, a balanced approach considering both human values and technological capabilities is required.

In summary, while generative AI creates complex challenges for the right to be forgotten, these challenges do not necessitate an outright rejection of the concept. With nuanced legal paradigms and ethical AI development, the societal benefits of these technologies can be harnessed while respecting human dignity and individual rights. As the digital landscape advances, maintaining this equilibrium must be the shared mission of legislators, regulators, technologists and civil society. The right to be forgotten provides a compass in this journey towards an ethical and empowering AI future guided by human values.