ISSN: 2755-9181

Review Article

Journal of Journalism and Media Management

Redacting The Past Online: The Right to Be Forgotten in Nigeria and Beyond

Opeyemi Caroline Babalola

University of Ibadan, Nigeria

***Corresponding author**
Opeyemi Caroline Babalola, University of Ibadan, Nigeria

Received: November 20, 2025; **Accepted:** December 04, 2025; **Published:** December 12, 2025

ABSTRACT

The permanence of digital information has given rise to the right to be forgotten, a legal innovation that seeks to balance privacy with public access to information. Online communities and search engines often perpetuate outdated or misleading records, leaving individuals vulnerable even after exoneration. Literature has examined this right in Europe, the United States, and parts of Africa, yet little attention has been given to its scope and enforceability within Nigerian law. This paper therefore explores the historical emergence, conceptual framework, and applicability of the right to be forgotten in Nigeria, with comparative insights from jurisdictions where the right is more developed. This study is doctrinal and desktop-based, relying on both primary and secondary sources. Primary sources include the Nigeria Data Protection Act (2023), the General Application and Implementation Directive (2025), the Constitution of the Federal Republic of Nigeria (1999 as amended), and judicial decisions such as Hillary Ogom v. Google LLC. Foreign precedents considered include Google Spain SL v. AEPD & González (2014), Olivier G v. Le Soir, and Karthick Theodore v. Registrar General (India). Secondary sources consist of journal articles, textbooks, theses, and official reports. The research found that while the right to be forgotten is gaining global traction, its application in Nigeria remains weak, hindered by conflicts with freedom of expression, limited judicial interpretation, and weak enforcement mechanisms. Territorial limitations and the public's right to information also restrict its practical scope. The study concludes that the Nigerian legal system must adopt clear guidance for courts and regulators, balancing privacy with competing rights. It recommends proportionality tests, anonymisation, and clearer statutory procedures to make the right to be forgotten more effective in practice [1].

Keywords: Digital Memory, Online Privacy, Data Erasure, Legal Innovation, Judicial Enforcement

Introduction

The popular saying that "the internet never forgets" underscores a critical reality of the digital age. The internet has an almost limitless capacity to store, reproduce, and retrieve information, often including details that individuals would prefer to remain buried. In many cases, online communities, such as the self-styled "diggers association", deliberately resurface such information for public consumption, regardless of the subject's wishes. This persistence of data may take the form of videos, photographs, documents, audio messages, or other digital records, all of which combine to create a near-permanent archive of personal lives. Confronting this reality has given rise to the concept of the right to be forgotten, an unpopular yet increasingly significant legal innovation.

The relevance of this right becomes clearer when certain events. About ten months ago, a teenager in Edo State was accused of poisoning her boyfriend and four of his friends [2]. The allegation spread rapidly across digital platforms, and even after she was cleared of all charges, the internet has not forgotten. A simple search of her name still associates her with the crime, and only two out of seven prominent search results reflect her exoneration. In such circumstances, the individual should reasonably have the right to dissociate her identity from the allegation. The central question, however, is how information that has already saturated the internet can be erased or corrected.

The most effective response lies in enforcing the right to be forgotten. Even in jurisdictions where it is not explicitly recognized, the right may be argued as an extension of the broader right to privacy. Since the landmark decision in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014), this right has attracted growing international recognition, and has shaped conversations on privacy and the permanence of digital memory [3]. Between July 2019 to December 2019, Google received over 925,944

Citation: Opeyemi Caroline Babalola. Redacting The Past Online: The Right to Be Forgotten in Nigeria and Beyond. J Journalism Media Manag. 2025. 1(1): 1-5. DOI: doi.org/10.61440/JJMM.2025.v1.28

content removal requests from Governments and courts in 19 countries [4]. According to Google, governments submit content removal requests for various reasons [5]. In some cases, authorities argue that certain material violates local laws and may attach court orders to their requests, even when such orders are not specifically directed at Google. Both types of requests are included in Google's transparency reports [6]. In addition, governments sometimes ask Google to review content to assess whether it breaches the company's community guidelines and content policies. Nigeria is not exempt from this process: since 2011, the country has made a total of 55 removal requests, identifying 297 items for removal [7].

This paper attempts an exposé on the right to be forgotten, how it came to fore, scope, practicability, limitations and applicability under Nigerian law in comparison with other jurisdictions while proffering recommendations for the Nigerian courts where this right will be determined.

Conceptual Framework

Definition of the Right to be Forgotten (Right to Erasure)

The right to be forgotten, as the name suggests, refers to the entitlement of individuals to have certain information about them erased, suppressed, or removed entirely from the internet. It empowers data subjects to compel the deletion of private information from search engines and online directories where such information is no longer relevant, or where the individual's privacy rights outweigh the public's interest in continued access [8]. Although the National Data Protection Act and the Nigeria Data Protection Regulation do not expressly define this right, its essence can be inferred from its application.

It is also commonly described as the right to erasure or de-listing, which allows individuals to request that search engines such as Google refrain from displaying results that contain outdated or harmful personal information. Importantly, this right does not always mean complete deletion; in some instances, it may extend to anonymisation of identifying details, as affirmed in Olivier G v Le Soir [9].

Definitions under the National Data Protection Act

The National Data Protection Act provides specific definitions that guide the interpretation and application of data protection principles in Nigeria. It defines a "data controller" as an individual, private entity, public commission, agency, or any other body who, alone or jointly with others, determines the purposes and means of processing personal data [10]. A "data controller or data processor of major importance" is described as a controller or processor domiciled, resident in, or operating in Nigeria who processes or intends to process personal data of more than such number of data subjects within Nigeria as the Commission may prescribe, or such other class of controller or processor whose processing is of particular value or significance to the economy, society, or security of Nigeria as the Commission may designate [11]. Similarly, a "data processor" is defined as an individual, private entity, public authority, or any other body, who processes personal data on behalf of, or at the direction of, a data controller or another data processor [12].

The Act further defines "personal data" as any information relating to an individual who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual [13]. A "data subject" refers to the individual to whom personal data relates, while a "personal data breach" means a breach of security of a data controller or processor leading to, or likely to lead to, the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed [14,15].

Clarification under the GAID

Beyond the NDPA, the General Administrative Implementation Directive (GAID) provides further clarity. It defines a "data subject access request" as a request directed to an organisation by a data subject, granting the latter the right to access information about the personal data being processed [16].

The Right to Be Forgotten in the Context of the Right to Privacy in the Pre-GDPR Era

Before the EU General Data Protection Regulation (GDPR) came into effect in 2018, the right to be forgotten had not yet been formally recognised in law. However, it was not entirely alien. It was often treated as a subset of the broader right to privacy, and there were instances under both national and international law where the right to privacy was interpreted in a manner that gave effect to what is now understood as the right to be forgotten.

Nigeria

In Nigeria, there is no judicial precedent that explicitly interprets the constitutional right to privacy as encompassing the right to be forgotten. However, The Constitution of the Federal Republic of Nigeria guarantees the fundamental right to private and family life in these terms: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected" [17,18].

While this provision has not yet been construed to include the right to be forgotten, the Supreme Court's obiter dictum in Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo suggests that such an interpretation may be feasible [19].

The Court observed

"The sum total of the rights to privacy and of freedom of thought, conscience or religion which an individual has, put in a nutshell, is that an individual should be left alone to choose a course for his life, unless a clear and compelling overriding state interest justifies the contrary." Following this dictum, it may be argued that an individual's right to be "left alone" necessarily includes the ability to control aspects of their existence online and to determine what personal information should reasonably remain outside the gaze of the public.

South Africa

In South Africa, section 14 of the Constitution guarantees the right to privacy in the following terms: "Everyone has the right to privacy, which includes the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed" [20].

Whether this provision can be reasonably interpreted to include the right to be forgotten remains subject to debate. In NM v Smith, the Court recognised that "it appears common cause in many jurisdictions that the nature and the scope of the right envisage a concept of the right to be left alone" [21]. Further guidance was provided in Bernstein v Bester, where Ackermann J identified three key principles underpinning privacy: that an individual can only assert privacy where there is a legitimate expectation of it; that privacy exists along a continuum, with stronger protection in intimate spaces and weaker protection in public ones; and that at its core lies the inner sanctum, which shields the most private aspects of personal life, thought, and autonomy [22,23].

India

Even before statutory recognition, Indian courts acknowledged the right to be forgotten as part of the broader right to privacy. This recognition can be traced back to Rajagopal v State of Tamil Nadu (1994), where the Court upheld the "right to be let alone," subject to exceptions for public documents and judicial records [24]. A landmark development came with the 2017 Supreme Court decision in Justice K.S. Puttaswamy v Union of India, which formally recognized the right to privacy as a fundamental right under the Indian Constitution [25]. In this case, Justice S.K. Kaul observed that the right of an individual to exercise control over their personal data and life "would also encompass his right to control his existence on the Internet." The Court acknowledged the right to be forgotten, emphasizing that it is not absolute. Illustrations were provided for situations where this right would not apply, including matters relating to public interest, public health, archiving, research, or legal claims. The judgment clarified that the recognition of the right to be forgotten implies that an individual should be able to remove personal data when it is no longer relevant or serves no legitimate purpose.

The Puttaswamy decision established an expansive interpretation of privacy: it is not merely a narrow right against physical intrusion, nor merely a derivative right under Article 21. Instead, it encompasses the body and mind, including personal decisions, choices, information, and freedoms. Privacy was held to be an overarching and enforceable right under Part III of the Constitution, multifaceted in nature, thereby implicitly supporting the concept of the right to be forgotten.

Europe

Prior to the Google Spain case and the introduction of the GDPR right to be forgotten, European courts had already addressed privacy issues in ways that laid the groundwork for these later developments. In 2004, the case von Hannover v Germany was instituted locally in Germany before eventually reaching the European Court of Human Rights [26]. The claimant, the eldest daughter of Prince Rainier III of Monaco, argued that several media outlets had published photographs of her and her family in locations where she had a legitimate expectation of privacy. She contended that the publication of these candid photos violated her right to privacy under the European Convention on Human Rights [27].

Relying on her status as a semi-public figure, the German courts held that her right to privacy was inherently diminished by her social position and authorized the publication of the photographs, emphasizing the freedom of the press and of expression. The Princess challenged this decision, arguing that the German tribunals had failed to adequately protect her privacy against mass media intrusion, thereby breaching Germany's positive obligations under both the national constitution and the European Convention on Human Rights.

The European Court of Human Rights reversed the German courts' decision. It reiterated that the concept of private life extends to aspects relating to personal identity, including a person's name and image. The Court held that "private life… includes a person's physical and psychological integrity," interpreting Article 8 as ensuring the development of each individual's personality without outside interference in their relations with others. This allowed the Court to conclude that there exists a "zone of interaction with others, even in a public context, which may fall within the scope of 'private life" [28].

Another illustrative case occurred in Belgium in 2016. In Olivier G v Le Soir, the Court of Cassation ordered a newspaper to anonymize the online version of a 1994 article concerning a fatal road traffic accident [29]. The applicant, who had been convicted of drink driving in connection with the accident, argued that his conviction was spent and that continued online publication of his name violated his right to privacy. The Court held that his privacy rights outweighed the newspapers and the public's right to information [30]. This shows the application of the "right to be forgotten" principle prior to the GDPR framework.

The Formal Recognition of the Right to Be Forgotten

The right to be forgotten was first expressly recognized by the European Court of Justice in the landmark case Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [31]. In this case, Mr. González, a Spanish resident, filed a complaint against Google Spain, Google Inc., and two Spanish newspapers. He argued that a search for his name on Google displayed information about a past property attachment that had long been resolved. He requested the removal of this information, as it was no longer relevant. The Court ruled in his favor, holding that the information should be erased from search results. This decision laid the foundation for the right to be forgotten in the EU and influenced similar developments in other jurisdictions.

General Data Protection Regulation (GDPR)

The right to be forgotten was codified in the EU General Data Protection Regulation (GDPR), which gives individuals the ability to request erasure of personal data without undue delay when any of the following grounds apply [32]:

1. The data are no longer necessary for the purposes for which they were collected or processed.
2. Consent on which processing is based is withdrawn, and no other legal ground exists.
3. The data subject objects to processing, and there are no overriding legitimate grounds for processing.
4. The personal data have been unlawfully processed.
5. Erasure is necessary to comply with EU or Member State law.
6. The data were collected in relation to information society services offered to a child.

Controllers who have made such data public must take reasonable steps to inform other controllers to erase links, copies, or replications of the data, taking into account available technology and cost.

The right to erasure under GDPR does not apply where processing is necessary: To exercise freedom of expression and information; To comply with legal obligations or perform tasks in the public interest or in official authority; For public health reasons; For archiving in the public interest, scientific, historical, or statistical research; or To establish, exercise, or defend legal claims [33].

Legal and Judicial Framework for the Right to Be Forgotten in Nigeria

In Nigeria, the right to be forgotten is recognized under the Nigeria Data Protection Act (NDPA), by granting a data subject the ability to request correction or, where correction is not feasible, the deletion of personal data that is inaccurate, outdated, incomplete, or misleading, as well as the erasure of personal data without undue delay [34,35]. The Act further obliges data controllers to erase personal data when it is no longer necessary for the purposes for which it was collected or processed, or where there is no other lawful basis for retaining it [36].

The 2025 General Application and Implementation Directive (GAID) further clarify the exercise of this right [37]. It establishes that personal data may be erased if it is no longer necessary, if consent is withdrawn, if an individual objects to processing justified on legitimate interest, if data is processed for direct marketing, if it was unlawfully processed, or to comply with a legal obligation [38]. However, the right is limited where processing is necessary to exercise freedom of expression, comply with legal obligations, perform tasks in the public interest or official authority, serve public health purposes, conduct research, or establish or defend legal claims [39]. Where data has been shared publicly or with third parties, controllers must take reasonable steps to ensure its erasure, while public interest considerations may override the right if the burden of proof lies with the controller [40].

The right has also been considered in Nigerian case law, notably in Hillary Ogom v Google LLC & Anor [41]. In this case, a cleric who had been convicted and imprisoned in the United Kingdom sought to compel Google to delete information regarding his conviction. He argued that the continued circulation of this information violated his rights to privacy, freedom of association, and human dignity, and hindered his employment prospects. The Court dismissed the action, finding that the claimant had not met the legal requirements to invoke the right to be forgotten. It has been suggested that the claim might have had a greater chance of success had it been grounded explicitly on the right to be forgotten and supported with evidence demonstrating that the continued retention of the data was legally unjustifiable. Notably, this case occurred in 2019, before the enactment of the NDPA, but the claim could have been constituted under Section 3.1 of the now-repealed Nigeria Data Protection Regulation, which similarly recognized the right to erasure.

South Africa

In South Africa, the right to be forgotten is not explicitly provided for in legislation, but it may be inferred from the Protection of Personal Information Act (POPI) [42]. Like many foreign data protection laws, POPI requires that personal information be stored and processed only to the extent that it is adequate, relevant, and not excessive in relation to its purpose [43]. The Act allows data subjects to request that responsible parties correct or delete their personal information or records [44]. Although there is no express law establishing the right to be forgotten, this provision is considered sufficient for practical purposes.

India

In India, the right to be forgotten is explicitly recognised under section he Digital Personal Data Protection Act, 2023, where it is referred to as the right to correction and erasure of personal data [45]. Under this provision, a Data Principal has the right to request correction, completion, updating, and erasure of personal data for which consent has previously been given, including consent under section 7(a) which defines consent as the voluntary, explicit, specific, and informed agreement of the Data Principal to allow the Data Fiduciary to process personal data for a clearly defined purpose [46,47]. Upon receiving such a request, a Data Fiduciary must correct inaccurate or misleading data, complete incomplete data, and update personal data. A Data Principal may also request the erasure of their personal data in a prescribed manner, and the Data Fiduciary must comply unless retention is necessary for a specified purpose or to comply with any law in force [48].

Complementing this, the Information Technology Rules, 2021, require intermediaries to remove or disable access to content infringing privacy within twenty-four hours of a complaint [49]. The Madras High Court in Karthick Theodore v Registrar General the Court addressed the appellant's request to redact his personal and intimate details from a publicly accessible judgment [50]. The appellant had been acquitted in 2014 of charges under Sections 417 and 376 of the Indian Penal Code. Years later, he sought to have his name and other identifying information removed from the judgment published online, citing the impact on his personal and professional life, including a denied Australian visa.

The Court recognized the right to be forgotten as an integral part of the constitutional right to privacy under Article 21 of the Indian Constitution and the right to be forgotten under the Digital Personal Data Protection Act. It emphasized that while courts are "Courts of Record" and preserve the sanctity of records, they are not obligated to make personal data publicly accessible. The Court directed the redaction of the appellant's personal details from the judgment and ordered that only the redacted version be available for publication, ensuring the full unredacted judgment remained part of the court's record [51].

Practical and Legal Barriers in the Enforcement of the Right to Be Forgotten

Territorial Limitation: While the right to be forgotten offers significant protections, it does not operate globally. Success in one country does not automatically guarantee the same result elsewhere. Its reach is generally confined to countries within the European Union, as reflected in the GDPR, which applies to processing personal data of individuals in the Union by controllers or processors outside the EU if the activity relates to offering

goods or services to such individuals or monitoring their behavior within the Union [52]. This limitation was highlighted in Google v Commission Nationale de l'Informatique et des Libertés (CNIL), where the ECJ reviewed a sanction imposed on Google by the French data protection authority for failing to remove content worldwide [53]. Google contended that removing content only from the French version of its search engine sufficed. The ECJ acknowledged the objective of the GDPR to ensure a high level of personal data protection across the EU but emphasized that many third states do not recognize the right to de-referencing or approach it differently. Consequently, the Court concluded that search engine operators are required to comply only for versions corresponding to EU Member States, using measures to prevent users from other states accessing the removed content [54].

Conflict with Other Rights-Freedom of Expression: The right to be forgotten is not absolute and must be balanced against other rights, such as freedom of expression. No right is inherently superior, and conflicts are assessed case by case. For example, in Smith v Daily Mail Publishing Company (US), a juvenile murder suspect challenged a newspaper's publication of his name under a West Virginia statute prohibiting such disclosure [55]. The US Supreme Court struck down the statute, holding that lawfully acquired information in the public interest could not be restricted, illustrating the limits of tort law and the primacy of constitutional free speech rights.

Public's Right to Information-Journalistic and Historical Interests: Accessibility of information is critical for research, due diligence, and public safety. For instance, online availability of a former convict's history may be necessary to prevent them from holding specific positions or protecting children from previously convicted sexual offenders. While this may feel punitive after a sentence is served, such consequences serve broader societal functions. Similarly, certain information may serve journalistic purposes or historical documentation. The relevance of personal data often depends on the individual's public position; information about political figures may be vital for public awareness, whereas data about private individuals, may hold limited public interest [56].

Recommendations

To strengthen the practical application of the right to be forgotten in Nigeria, NITDA and the NDPC should develop and issue clear, practical guidance on its implementation. This guidance should cover key areas such as erasure, delisting, and anonymisation of personal data, specifying timelines for compliance and clarifying the law's scope in cross-border situations. By providing structured procedures, these agencies can help data controllers, courts, and individuals navigate the right effectively and consistently. Additionally, courts should adopt a proportionality test when adjudicating cases involving the right to be forgotten. This test would carefully balance the individual's privacy rights with freedom of expression, public interest, and the economic rights of creators. In cases where full deletion of data is disproportionate, courts should consider anonymisation or partial redaction as a fair compromise that protects privacy without unnecessarily restricting access to legitimate information.

Conclusion

While the internet may never forget, a robust legal framework and balanced judicial approach can ensure that individuals are not perpetually defined by their past. Clear rules and consistent enforcement can create an environment where privacy is respected without stifling public discourse or access to information. As Bruce Schneier wisely observed, "Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect." By embedding this principle into both law and practice, Nigeria can move closer to a system where the right to be forgotten serves as a meaningful tool for protecting personal dignity in the digital age.

Reference

1. Case, Judgment of the Court (Grand Chamber). 2014. 317.
2. 'Number of government and court requests for content removal from Google in 2nd half of 2023, by region'. 2025.
3. Google, 'Government removal requests by the numbers: Nigeria' (Transparency Report, Google). 2025.
4. Emmanuel Ikwuakolam, 'X-Raying the Legal Framework for Enforcement of the Right to Be Forgotten in Nigeria'. 2025.
5. Olivier G v Le Soir. 2016.
6. National Data Protection Act. 2023. 65.
7. General Administrative Implementation Directive, art. 52.
8. Constitution of the Federal Republic of Nigeria. 1999. 37.
9. Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo. 2001.
10. Constitution of the Republic of South Africa. 1996. 14.
11. NM and Others v Smith and Others. 2007. 250.
12. Bernstein and Others v Bester NO and Others. 1996. 2.
13. Rajagopal v State of Tamil Nadu. 1994. 632.
14. Justice KS. Puttaswamy v Union of India. 2017. 1.
15. Von Hannover v Germany. 2004. 21.
16. European Convention on Human Rights, art. 1950. 8.
17. Von Hannover V. Germany. E.M.L.R. 2004. 21.
18. Olivier G v Le Soir. n°. 2016.
19. European Convention on Human Rights. 1950. 10.
20. Regulation (EU) of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. 17.
21. Nigeria Data Protection Act. 2023.
22. The General Application and Implementation Directive (GAID). 2025. 38.
23. Protection of Personal Information Act. 2013.
24. Digital Personal Data Protection Act. 2023. 12.
25. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules India. 2021.
26. Regulation (EU) of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. 3.
27. Inibehe Effiong. 'The Right to Be Forgotten Under the Data Privacy & Data Protections Laws'. 2025.