JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOLUME 10 • ISSUE 1 • 2019

– NOTE –

FORGET ME, FORGET ME NOT: ELEMENTS OF ERASURE TO DETERMINE THE SUFFICIENCY OF A GDPR ARTICLE 17 REQUEST

Haya Yaish[1]

ABSTRACT

The data subject's (or the individual to whom the data relates) right to erasure under the new EU's data protection law is likely to cause tensions with the right to freedom of expression. Using Article 17(1)(d)-(e) of the General Data Protection Regulation as a nexus to trigger and apply the right to privacy in EU law to the right to erasure, this Note presents a balancing test of four factors that can be used to consistently determine whether individual cases that request a right to erasure for published material are entitled to privacy protections. The proposed balancing test "Elements of Erasure" asks the following questions regarding the published information: whether there was a reasonable expectation of privacy, whether there was a reasonable expectation of a duty of confidence, how the information was collected, and whether an individual is personally identifiable using the disclosed information.

Keywords: Data protection, data privacy, freedom of expression, GDPR, information privacy, internet, regulation, right to erasure

[1] J.D. Candidate 2019 at George Washington University Law School.

CONTENTS

INTRODUCTION

Should individuals have the right to ask Google or a local newspaper to erase pictures, descriptions, or audio of themselves in certain circumstances? Should individuals feel differently about unflattering pictures taken after winning their elementary school's spelling bee or pictures of them partying on spring break? What rights do individuals have regarding pornographic videos of themselves posted online? Should their rights differ if the pornographic material is revenge porn? Should individuals be able to erase their mugshots after they got arrested for public intoxication in college? What if the information posted online relates to the number of steps an individual took one day and posted online through a health tracker, and then subsequently found the information displayed on an unrelated blog post? Should the individual have a right to remove the information from being displayed to the public?

Assume that an individual witnessed a crime in public and their picture was plastered all over the news. Should that individual have legal protections to prevent the images from being displayed although the individual is only in the pictures' background and saw the photographers? Would individuals generally feel differently about pictures of their toddlers being published globally? What if an individual's famous long-term ex is detailing everything humiliating the individual has done in an autobiography, does it matter if a pseudonym is used for the person's name? What about publishing a private conversation an individual had in public?

Privacy laws are rapidly emerging and developing, yet remain a relatively unstructured area of law with vast global disparities in both legislation and common law.[2] The European Union General Data Protection Regulation (GDPR), coming into force in mid-2018, will radically change the data privacy climate. Article 17 of the GDPR, the right to erasure (RTE), which is synonymous with the right to be forgotten (RTBF) for this Note's purposes, allows the erasure of personal data under specific circumstances.[3] Article 17 is often considered vague or unclear in certain aspects, particularly when it conflicts with the right to freedom of expression. This Note aims to clarify, based on international law, common law, and notions of privacy, when privacy should prevail over the right to free expression, justifying an individual's right to erasure.

This Note generates a balancing test that will be termed "elements of erasure (EOE)." This test proposes factors courts and practitioners can use to evaluate and allow or deny an Article 17 RTE request when individuals request the erasure of published "private information" and the cases do not explicitly fall under the clear circumstances that warrant or prevent erasure in sub-articles (1)(a)-(e)[4] or when the cases may conflict with sub-article(3)(a)[5]. These factors list the relevant elements

[2] *Compare* UAE Federal Decree-law no.5/2012 dated 13/08/2012 AD On Combating Cybercrimes, http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf, *with* Laws of Malaysia, Act 709, Personal Data Protection Act 2010, http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf (contrasting UAE and Malaysian privacy laws that protect varying interests); Jackson Lewis PC, Alabama Senates Passes Data Breach Notification Act, Lexology (Mar. 6, 2018), https://www.lexology.com/library/detail.aspx?g=9e5a0747-faa9-4400-95fc-d5ffe4891d05, *and* Cal. Civ. Code §1798.82 (amended by Stats. 2016, Ch. 337, Sec. 2. (AB 2828)), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82 (contrasting the large disparities in state data breach notification laws).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. [hereinafter GDPR], https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679.

[4] *Id*. at art. 17(1)(a)-(e).

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

of privacy in the context of publishing personal information and freedom of expression, and aim to clarify which information is considered private under the right to erasure, thus permitting its erasure under the GDPR's RTE in accordance with the European Charter of Human Rights and the Charter of Fundamental Rights of the European Union. The EOE conceptualize elements of privacy by analyzing English common law, cases decided by courts including the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), and various scholars' arguments and theories.[6]

Part II of this Note discusses background information including an influential case, the Data Protection Directive, the GDPR and Article 17, EU laws pertaining to the right to freedom of expression and the right to privacy. Part II also discusses the meaning of privacy and provides the necessary background to build a foundation for the "elements of erasure." Part III discusses unresolved ambiguities within the GDPR, examines tensions between the right to freedom of expression and the right to privacy, analyzes data privacy court decisions, and presents the balancing test coined, "elements of erasure," to assess RTE requests comprehensively and ensure individual privacy protections and control of personal data and information without stifling the freedom of expression and information.

A few important notes regarding the topic and scope of this Note: 1) This Note rests on the assumption that the RTE should be based on the right to privacy in EU law as implied in Article 17(1)(d)-(e); 2) when discussing erasure, this Note refers to the simple erasure of data: the technical delisting, delinking, or removal of data being displayed; 3) the EOE aim to provide a solution for individual cases with Article 17 requests that do not neatly fall under Article 17(1)(a)-(c),(f) and 17(3)(b)-(e) which state clear circumstances that warrant erasure such as withdrawal of consent or clear circumstances that prohibit erasure such as established public interest purposes or legal obligations; and 4) the EOE do not discuss nor consider cases with Article 17 requests as a result of the publication of mass data and private information or data breaches.

I. BACKGROUND

[6] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 67 (2008) (stating that a theory of privacy should be pluralistic, should be general but not too vague, and should accommodate the dynamic nature of privacy while maintaining widespread applicability. A theory of privacy, therefore, should consist of a framework for identifying the plurality of things that fall under the rubric of privacy. The framework must be concrete, but not so context-specific as to prevent wide application.)

In a landmark case against Google Spain, a man successfully sued Google to remove an unfavorable link concerning himself, an outcome that changed the way we perceive the role of search engines in our society. This case has implications on privacy and the freedom of information in general, and in particular, stirs the debate on whether, and if so when, individuals can request the removal of personal information from the public realm. This section delves into the details of Google Spain v. AEPD to better understand the implications of the decision on the RTE, the laws the case was based on; the EU Data Protection Directive, the GDPR and Article 17, followed by an explanation of EU privacy and freedom of expression laws. Different understandings and conceptualizations of privacy culminate this section.

A. Google Spain v. AEPD

In 2014, a Spanish citizen prevailed in his complaint against a Spanish daily newspaper, Google Inc., and Google Spain after a portion of his complaint sought to remove or alter pages that depicted a forced real-estate auction as a result of attachment proceedings from social security debts.[7] He argued that the pages were irrelevant given that the proceedings were resolved.[8] The CJEU outlined features that were used to assess the data's compatibility with the directive[9] and considered the interference of this information with elements of his private life,[10] "the legitimate interest of internet users potentially interested in having access to that information," "the nature of the information in question and its sensitivity for the data subject's private life," "the role played by the data subject in private life," whether the data is relevant or not, and whether the data was "excessive in relation to the purposes for which they were processed."[11] Ultimately, the court ruled that the RTBF may apply even when data has been lawfully processed if the data is "inadequate, irrelevant or no longer relevant, or excessive in relation to those

[7] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 93.
[8] *Id*. at ¶ 15.
[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) [hereinafter EU Data Protection Directive], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.
[10] Court of Justice of the European Union, Press Release No 70/14, Judgment in Case C-131/12 (2014), https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (stressing that "the effect of the interference with the person's rights is heightened on account of the important role played by the internet and search engines in modern society").
[11] *Id*.

purposes and in the light of the time that has elapsed."[12] The court also explained that the RTBF is not an absolute right and must be weighed against other legitimate interests and rights.[13]

Although the court ruled that Google, as an internet search engine, should comply with requests to remove private information that meets the standards the court outlined, the court did not order the newspaper to remove the information too.[14] This element has perplexed scholars, and has not been explained by the court other than stating that it was published lawfully.[15] The court also stated that the search engine's activities include collecting, retrieving, recording, organizing, storing, and disclosing data, which makes the search engine a data controller.[16] As a data controller, Google is subject to the Data Protection Directive (the Directive) (the current EU data protection law that precedes the GDPR), meaning that the court effectively ruled that the search engine operator must comply with the Directive and remove the personal information from the search results as requested by the data subject.[17] This was a highly controversial decision which lead to widespread debates over the right to be forgotten and its effect on the freedom of expression.[18]

While this decision was heavily applauded, it was also widely criticized and viewed as a restriction to the freedom of speech and expression. One way to phrase the CJEU ruling is by saying it has "interpreted the Directive as creating a presumption that Google must delete links to personal information from search results at the request of a data subject unless a strong public interest suggests

[12] Google Spain SL v. AEPD, at ¶ 93.
[13] *Id*. at ¶ 86.
[14] *See id*.; The Right to Be Forgotten (Google v. Spain), ELECTRONIC PRIVACY INFORMATION CENTER (Apr. 7, 2018), https://epic.org/privacy/right-to-be-forgotten; *see also Google Spain SL v. Agencia Española de Protección de Datos*, 128 HARV. L. REV. 735 (Dec. 10, 2014) [hereinafter *Google Spain*], http://harvardlawreview.org/wp-content/uploads/2014/12/google_spain_sl_v_agencia_espanola_de_proteccion_de_datos.pdf.
[15] *Google Spain*, at 736. *See generally* David Hoffman, Paula Bruening & Sophia Carter, *The Right to Obscurity: How We Can Implement the Google Spain Decision*,17 N.C. J. L. & TECH. 437 (2016), http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1302&context=ncjolt (analyzing the application of this opinion and explaining that it does not result in "forgetting" any of the information, but obscuring the information).
[16] Google Spain SL v. AEPD, at ¶ 28.
[17] *Google Spain*, at 735.
[18] *See* Alan Travis & Charles Arthur, *EU court backs 'right to be forgotten': Google must amend results on request*, THE GUARDIAN (May 13, 2014), https://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results (highlighting EU justice commissioner Viviane Reding's support for the court's decision); *see also* Jonathan Zittrain, *Don't Force Google to 'Forget'*, N.Y. TIMES (May 14, 2014), https://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html (arguing that the court's decision is both too broad and too narrow and is a form of censorship).

otherwise."[19] Critics argue that this interpretation places too much power and control of public information in the hands of private entities, arguing that the court interpreted the Directive incorrectly when they broadened the interpretation of a data controller and found Google to be a controller, not a processor, based on having a search algorithm, although the search engine does not produce and publish its own content.[20] This case also raises questions regarding the scope of data controllers' legal and ethical responsibility in controlling information, and the excessive requests of erasure that are likely to arise given that the data subject may object to the display of their data even if the data is not prejudicial.[21] Another criticism is that the court prioritizes privacy rights which limits access to information and allows individuals to impede such access without providing adequate protections to the public interest and freedom of expression.[22] Despite these valid criticisms and an unclear opinion by the CJEU, the court's decision that prioritizes privacy rights and grants power to data controllers stems from Article 7 and Article 8 of the Charter,[23] and the Directive which states that "it shall be for the controller to ensure that [principles relating to data quality including fair, lawful, accurate, and relevant processing and collection] is complied with." [24]

B. EU Data Protection Directive

The Google Spain case was based on the EU Data Protection Directive (Directive 95/46/EC) Articles 12 (b) and 14 (a),[25] however, the General Data Protection Regulation (GDPR) will supersede Directive 95/46/EC.[26] The GDPR was approved by the EU Parliament on April 14, 2016 and will come into effect on May 25, 2018.[27] The GDPR aims to "harmonize data privacy laws across Europe,

[19] *Google Spain*, at 735.
[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] Charter of Fundamental Rights of the European Union, art. 7-8, 2010 O.J. (C 83/02), [hereinafter Charter of Fundamental Rights], http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[24] EU Data Protection Directive, *supra* note 8, at art. 6.
[25] *Id*.; *See* Margaret Rouse, *EU Data Protection Directive (Directive 95/46/EC)*, WHATIS, http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC (last updated January 2008) (stating that "the EU Data Protection Directive is based on recommendations proposed by the Organisation for Economic Co-operation and Development (OECD)"); *See also* Org. for Econ. Co-operation and Dev. (OECD), *The OECD Privacy Framework* (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[26] EU GDPR.ORG, https://www.eugdpr.org/ [https://perma.cc/52MU-CTMR] (last visited October 21, 2018).
[27] *Id*.

to protect and empower all EU citizens data privacy and reshape the way organizations across the region approach data privacy."[28] The origins of data privacy laws in the EU stem from the Organisation for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which advanced principles for the protection of personal data and the right of privacy.[29]

C. GDPR and the Right to Erasure

As seen in EU case law and Directive 95/46/EC, the RTBF or RTE is not a novel concept. Additionally, the GDPR dedicates an entire Article to the concept "right to erasure ('right to be forgotten')," further clarifying and expanding its role in EU privacy law. However, many elements and sections of the law remain unclear, and more questions arise when we analyze the practical implications of this Article.[30] The full text of Article 17 of the GDPR, titled "Right to erasure ('right to be forgotten')" is provided at the end of this Note in Appendix A.

D. EU Privacy and Freedom of Expression Laws

Privacy laws and freedom of expression laws are not opposing forces in all circumstances; privacy laws are often necessary to protect an individual's freedom of expression. However, RTE requests may be argued to have a chilling effect on the freedom of expression and information. To reach a recommendation that achieves to balance both interests, which will be presented in the analysis section, EU privacy laws and freedom of expression laws are delved into below.

1. Privacy Laws

[28] *Id.*
[29] *See* EU GDPR.ORG, *How Did We Get Here? An Overview of Important Regulatory Events Leading up to the GDPR*, https://eugdpr.org/the-process/how-did-we-get-here/ [https://perma.cc/GAF5-YAAJ] (last visited Apr. 7, 2018) (listing the OECD's proposed principles for protecting personal information: (1) Collection Limitation Principle; (2) Data Quality Principle; (3) Purpose Specification Principle; (4) Use Limitation Principle; (5) Security Safeguards Principle; (6) Openness Principle; (7) Individual Participation Principle; and (8) Accountability Principle.); s*ee also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017 255-56 (2017) [hereinafter SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017] (explaining additional concepts the OECD added to the original eight key principles in 2013 which include national privacy strategies, privacy management programs, and data security breach notification).
[30] *See infra* Section III.

Although an underdeveloped area of the law, privacy law is more advanced in Europe than elsewhere in the world. Even prior to the GDPR, the right to privacy has an indisputable place in EU law, unlike the United States' constitutional right to free speech which is more likely to trump the right to privacy.[31] Most notably, individuals have certain privacy rights under the law. The Charter of Fundamental Rights of the European Union (the Charter), Article 7 states that "[e]veryone has the right to respect for his or her private and family life, home and communications,"[32] and Article 8 states that "[e]veryone has the right to the protection of personal data concerning him of her," and that "[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[33] The Google Spain decision hinged on the Charter as the court stated that the data subject may request the erasure of his information based on Articles 7 and 8, and states that those rights override both the economic interest of the search engine and the interest of the general public in having access to the information.[34] The court then stated that the exception to this protection is when the role played by the data subject in public life justifies the preponderant interest of the general public having access to the information.[35]

Furthermore, the first legally binding treaty addressing data privacy is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as the Council of Europe Convention on Privacy.[36] It is a non-self-executing treaty to which forty-six countries have acceded, and requires signatory nations to create data protection legislation that provides safeguards for processing personal information that achieve the minimum levels of protection specified in the convention.[37] Finally, Article 8 of the European Convention on

---

[31] *See* U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").
[32] Charter of Fundamental Rights, *supra* note 22, at art. 7.
[33] *Id*. at art. 8.
[34] Case C-131/12, Google Spain SL v. AEPD, 2014 E.C.R. 317, ¶ 99.
[35] *Id*.
[36] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108, https://rm.coe.int/1680078b37 [https://perma.cc/P8RG-ZRPA]; *see* SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017, *supra* note 28, at 259.
[37] *See* SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017, *supra* note 28, at 259-60 (noting the importance of Article 5 of the Convention on "data quality" and its relevance to Federal Information Processing Standards (FIPs), the authors state: "In its broadest sense, data

Human Rights (the Convention) titled "right to respect for private and family life" states that everyone has the right to private family life, and prohibits a public authority from interfering with this right except for reasons in accordance with the law and necessary in a democratic society that pertain to national security, public safety, the country's economy, criminal and public health purposes, or for protecting the rights and freedoms of others.[38]

Moreover, the Directive Articles 2, 4, 12, and 14 cover relevant definitions and the data subject's right including the data subject's right of access to data in three circumstances;[39] the first relates to timely access and prohibits excessive delays, the second involves the rectification, erasure or blocking of inaccurate or incomplete data that does not comply with the Directive, and the third dictates the need to notify third parties whose data has been affected in particular circumstances unless impossible or involves a disproportionate effort.[40] The Directive also covers the data subject's right to object to the processing of personal data in a particular situation when justified, and the right to be informed of and object to personal data disclosures when the data subject's personal data is being disclosed to or used by third parties for the purposes of direct marketing.[41]

The right to privacy in the EU stems from a culmination of these various sources. The Directive highlights an individual's right as a data subject and the handling of the data subject's information. The GDPR further builds on the Directive, expanding the data subject's rights while clarifying ambiguous sections. However, the general right to privacy is rooted in the Charter, unambiguously declaring privacy as an uncompromising right held by all individuals within the EU. The Conventions complement the Charter by providing minimum protections for the general right to privacy. Together, the EU's framework for the individual's right to privacy is superior to any other country or region.

2. Freedom of Expression Laws

quality requires that personal information be 'stored for specified and legitimate purposes and not used in a way incompatible with those purposes.' Moreover, the concept of data quality limits the processing of personal data to circumstances that are 'adequate, relevant and not excessive in relation to the purposes for which they are stored.'").

[38] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4 1950, E.T.S. No. 5, https://rm.coe.int/1680063765 [hereinafter European Convention on Human Rights].

[39] EU Data Protection Directive, *supra* note 8, at art. 2, 4, 12 and 14.

[40] *Id*. at art. 12.

[41] *Id*. at art. 14.

Article 10 of the European Convention on Human Rights (the Convention) is the main source of law declaring the right to freedom of expression in the EU. The Convention specifies that the right to freedom of expression includes the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."[42] However, the right to freedom of expression is not limitless. As the second section of Article 10 goes on to state, these freedoms may be subject to conditions or restrictions under the law that are necessary in a democratic society, in the interests of national security, territorial integrity, public safety, preventing crime, protecting health, morals, reputation or rights of others, preventing disclosure of confidential information, and maintaining an impartial judiciary.[43] The Article, outlining the right to freedom of expression, clarifies that the exercise of this freedom may be subject to necessary restrictions in the interest of the right to privacy "for the protection of the reputation or rights of others" and "for the disclosure of information received in confidence."[44] Unlike US law, European legislators and courts may interpret this law as a requirement to balance the right to expression with the right to privacy.

E. Scholars' Recommendations for Resolving Privacy and the Freedom of Expression

Many scholars have provided recommendations on means to resolve tensions between the RTBF and the freedom of expression. Edward Lee provides numerous suggestions for resolving these tensions. He suggests trumping one right in favor of the other, but explains the potential dangers of doing so, which include severely limiting one right.[45] He also suggests a presumption in favor of one right. However, when a presumption is strong, it may have the same consequence as trumping one right, resulting in an ineffective strategy for balancing both rights.[46] He further suggests cataloging and enumerating the outcomes of certain factual situations.[47] While seemingly reasonable and practical, this recommendation may overlook important distinct circumstances. However, he further suggests that the enumerated factors could be considered as presumptions subject to exceptions

[42] European Convention on Human Rights, *supra* note 37, at art. 10.
[43] *Id*.
[44] *Id*.
[45] Edward Lee, *The Right to Be Forgotten v. Free Speech*, 12 I/S: J.L. & POL'Y FOR INFO SOC'Y 85, 98-99 (2015).
[46] *Id*. at 100.
[47] *Id*.

which is an adequate solution that is more likely to produce fair results.[48] However, a case-by-case assessment of the facts is still warranted in this case, and the catalog must be consistently updated as technology develops rapidly and increases in complexity. Lee ultimately recommends that Google work with policy makers to allow for the deletion of embarrassing photographs and expunged convictions of minors on social media. Recognizing similar rights for adults, Lee recommends de-ranking search results.[49] This suggestion will heavily increase the administrative burden and increase the number of frivolous cases. Recognizing such rights for adults would likely to limit access to public information and lead to unnecessary litigation over what constitutes an "embarrassing" photo.

Shaniqua Singleton has suggested recommendations that can be implemented by the private sector.[50] She states that clear standards can be set to inform companies when they should honor individuals' removal requests.[51] Having uniform standards is a practical solution, but agreeing on the standards that require the removal of information is difficult given the varying factual circumstances of each case. Also, RTEs are likely to increase significantly since individuals will no longer have to file suits to remove their data, imposing severe administrative burdens on search engines. Further, the uniform standards are likely to be broad and widely-applicable, thus potentially decreasing the public's access to information and limiting the freedom of expression.

Furthermore, David Hoffman, Paula Bruening, and Sophia Carter authored an article that deals with implementing the Google Spain decision.[52] Among other recommendations, they suggest using six criteria to evaluate individuals' requests to remove links to protect "an individual's right to obscurity:" lapse of time, illegally obtained data, discrimination, sensitive data, taken out of context, and individual as victim.[53] Although the factors approach the requests holistically, many factors rest on the assumption that an individual's right to privacy is triggered by negative consequences arising from the publication of private information. However, the right to privacy is not extinguished when the publication of private information does not subsequently harm the individual.

F. Reconciling Historical Definitions of Privacy with the Law of Privacy

[48] *Id*. at 101.
[49] *Id*. at 110.
[50] Shaniqua Singleton, *Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD*, 44 GA. J. INT'L & COMP. L. 165, 191-93 (2015).
[51] *Id*.
[52] David Hoffman, Paula Bruening & Sophia Carter, *The Right to Obscurity: How We Can Implement the Google Spain Decision*, 17 N.C.J.L. & TECH. 437 (2016).
[53] *Id*. at 478-80.

To be able to understand nuances in privacy law and the contention in defining what is private and entitled to the RTE, a general understanding of conceptualizations of privacy in the legal environment is necessary. A brief introduction and summary comprising different understandings of the definition of privacy are listed below, followed by a brief and limited introduction to the history of privacy law as well as two prominent common law privacy concepts. Understanding common law privacy concepts lends to further distinguishing contentious areas in privacy law and helps better analyze the treatment of data privacy law cases.

1. **What is Privacy?**

The general view of privacy is often too limited because people tend to search for a core characteristic to define privacy. Many scholars have proposed such characteristics and other theories and criticisms associated with defining privacy.[54] To fully understand the EOE, privacy and its underlying components must be presented through a variety of definitions, approaches, and conceptualizations. The internet adds an extra layer of complexity to the task of conceptualizing privacy because the rapidly changing and advancing technology makes it difficult to create legal solutions that anticipate novel threats to privacy. Professor Paul Schwartz describes critical challenges and essential factors that impact privacy, particularly the unparalleled ways information technology and cyberspace affect individual self-determination and democratic deliberation.[55] Samuel Warren and Louis Brandeis, as discussed below, argued that privacy is the right "to be let alone."[56]

The traditional and most common way to define privacy is to look at how the word "privacy" is used and construct a category with clear boundaries of what falls within and what falls outside the definition of privacy.[57] This method arguably limits the definition of privacy as it champions a binary approach to privacy that does not accurately reflect complicated facts of everyday life. Another common understanding of privacy equates privacy with secrecy, and finds that privacy is

[54] *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008); Anita L. Allen, *Coercing Privacy*, 40 WM & MARY L. REV. 723 (1999); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978).
[55] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999). *See also* Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000).
[56] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).
[57] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1096 (2002).

violated when secret or concealed information is publicly disclosed.[58] Control over personal information is another conceptualization of privacy, but it is argued to be too narrow and only a subset of privacy because it excludes private matters unrelated to personal information, such as the right to make reproductive decisions.[59] Professor Daniel Solove argues that referring to privacy in the abstract is usually not useful in practice, and should be defined in particular contexts to make the concept digestible.[60] Further, Professor Solove states that the means of conceptualizing privacy influences the legal solutions that are provided to solve specific problems.[61]

2. **History of Privacy Law**

Samuel Warren and Louis Brandeis are arguably the discoverers of privacy law.[62] In the late nineteenth century, developments in the media such as sensationalistic scandalous news being printed in "penny presses," and instantaneous photography as a result of Kodak's "snap camera," quickly contributed to disseminating information that was generally considered private in the public realm.[63] Warren and Brandeis authored their infamous article "The Right to Privacy" during this period and recognized these technological developments as challenges to privacy.[64] In their influential article, Warren and Brandeis argued for a new right to privacy, because existing laws such as contract law or defamation law were not sufficient for protecting privacy rights.[65] They further argued that the law should embrace and recognize the right to an "inviolate personality."[66] They derived a right to privacy or the right "to be let alone" from an English common law case called *Prince Albert v. Strange*.[67] While the *Prince Albert* case centered on the law of confidentiality, rather than privacy, Warren and Brandeis argued that the law of privacy already existed, making them mere "discoverers" of privacy law,

[58] *Id*. at 1105.
[59] *Id*. at 1110.
[60] *Id*. at 1154.
[61] *Id*.
[62] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 11 (6th ed. 2018).
[63] *Id*.
[64] *Id*.
[65] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197, 211 (1890).
[66] *Id*. at 205-06, 211.
[67] *Id*. at 195, 204.

rather than its inventors.[68] By 1903, the courts created privacy torts tailored to the harms Warren and Brandeis note in their article.[69]

3. **Common Law Privacy Concepts**

Two common law approaches to privacy laws are first, Prosser's privacy torts, which were born out of a law review article authored by William Prosser that built on Warren and Brandeis' law review article, and second, the law of confidence, an equitable doctrine in English law that sprouted from *Prince Albert*, a case decided by the High Court of Chancery in England in 1849,[70] and discussed in Warren and Brandeis' article. [71]

William Prosser's famous article, titled Privacy, contends that the law of privacy is based on four different types of invasion of a person's interests.[72] He argued that the only element privacy tort cases have in common is their effect on the plaintiff's right "to be let alone,"[73] and described the four privacy torts as: "1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; 2) public disclosure of embarrassing private facts about the plaintiff; 3) publicity which places the plaintiff in a false light in the public eye; 4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[74] While scholars have responded differently to Prosser's article,[75] Prosser's framework solidified and

[68] *Id*. at 213.
[69] SOLOVE & SCHWARTZ, *supra* note 61, at 25.
[70] *Prince Albert v. Strange*, 1 Mac & G 25, 1171 (1849) (holding that "the right and property of an author or composer of any work, whether of literature, art, or science, in such work unpublished and kept for his private use or pleasure, entitles the owner to withhold the same altogether, or so far as he may please, from the knowledge of others; and the Court will interfere to prevent the invasion of this right by the publication of a catalogue containing a description of such work").
[71] Warren & Brandeis, *supra* note 64, at 202, 204, 208.
[72] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
[73] *Id*.
[74] *Id*.
[75] *See e.g.*, Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 991, 1000-01 (1964) (responding to Prosser's view on privacy tort cases by stating "[i]n Dean Prosser's view the interest vindicated in each of these classes of cases is a different one. In my view the interest protected in each is the same, it is human dignity and individuality, or in Warren and Brandeis' words, 'inviolate personality'."); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Cal. L. Rev 957, 957 (1989) (presenting his view on the purpose or privacy torts by arguing that "the common law tort of invasion of privacy safeguards social norms, which he calls 'rules of civility,'" and that is based on the assumption that "personality, as well as human dignity, are injured by the violation of these norms"); Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887, 1922 (2010) (stating that "tort privacy became rigid and static" after Prosser).

organized the law of privacy in the United States, with the Restatement of Torts recognizing Prosser's four torts.[76]

On the other hand, the common law tort of privacy in England is rooted in the law of confidence which is based on the implicit contract of confidentiality.[77] The law of confidence holds "that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent."[78] Further, common law provides that there are three circumstances allowing the disclosure of confidential information: first, "where the individual to whom the information relates has consented," second, "where disclosure is in the public interest," and third, "where there is a legal duty to do so."[79] The breach of confidence doctrine is constantly changing and developing to "reflect changes in society, technology and business practice."[80] For a successful civil claim action of breach of confidence, the information has to have "the necessary degree of confidence about it, the information was provided in circumstances importing an obligation of confidence, and (for an injunction of declaration to be granted), there was an unauthorized use or disclosure of that information and, at least, the risk of damage."[81]

II. ANALYSIS

The Directive's RTBF tensions with the freedom of expression has been noted and discussed widely. As a result, the GDPR aims to extinguish some tensions by outlining areas in which the right to privacy is unlikely to prevail in Article 17(3)(b-e) (the exceptions). However, some ambiguities can only be resolved once they are litigated in court. Below, assumptions and clarifications made for this Note's purposes are explained and tensions between Article 8 and Article 10 of the Convention are assessed closely, followed by an analysis of the treatment of privacy cases by EU courts to identify important issues that determine what information is private and entitled to the RTE. Lastly, this Note proposes the EOE, a new test that courts can use to help determine whether information is private and entitled to the RTE in a consistent, fair, and comprehensive manner.

---

[76] SOLOVE & SCHWARTZ, *supra* note 61, at 28.
[77] UK DEP'T OF HEALTH, THE COMMON LAW DUTY OF CONFIDENTIALITY, http://webarchive.nationalarchives.gov.uk/+/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_5803173 (last visited Apr. 7, 2018).
[78] *Id.*
[79] *Id.*
[80] Douglas v. Hello! Ltd. [2000] EWCA (Civ) J1221-14 [165], [2001] QB 967.
[81] UK HEALTH AND SAFETY EXEC., BREACH OF CONFIDENCE, http://www.hse.gov.uk/enforce/enforcementguide/court/reporting-breach.htm (last visited Apr. 7, 2018).

A. Unresolved Ambiguities in Article 17

There are unresolved ambiguities within Article 17 of the GDPR that will be challenged and clarified when the law is enforced. But to be able to suggest EOE, this Note presents the approach that was used to handle the vague areas within the law.

The definition of "controller" remains to be a point of contention in cases concerning the publishing of individual information. Article 17 starts with declaring the data subject's right to the erasure of personal data from the "controller".[82] While a "controller" has been defined in the GDPR,[83] it is not as clear to identify the "controller" as it would be in cases where data is systematically being collected by an entity for specific or general purposes. For example, prior to Google Spain, it was initially unclear whether Google was considered to be only a processor of information or a controller of information. This is significant because controllers have increased duties under the law. The controlling precedent in this area comes from the German Federal Court of Justice case of Google Autocomplete.[84] The court held that having the plaintiff's business name associated with the words "scientology" and "fraud" in Google's "autocomplete" function despite no connection to fraud or scientology consisted of a personality right violation, and ruled that the autocomplete function was Google's content.[85] The court held that Google had a responsibility "to prevent their software from generating a result that would lead to the privacy violation" even though it was not required to ensure that the software and autocomplete suggestions would not violate privacy rights in advance.[86] Based on the Google Autocomplete decision, this Note assumes that "controllers" are both internet search engines and individual or institutional publishers as the court ruled that search engines are capable of

[82] GDPR, art. 17. (1).
[83] *See* GDPR, art. 4 ("'[C]ontroller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union of Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.").
[84] Bundergerichtshof [BGH] [Federal Court of Justice] May 14, 2013, ENTSCHEIDUNGEN DES BUNDERGERICHTSHOFES IN ZIVILSACHEN [BGHZ] 2, 2013 (Ger.).
[85] *Id.*
[86] SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017, *supra* note 28, at 263.

producing their own content through autocomplete and algorithms.[87] Consequently, I will extrapolate this decision and assume that controllers have the capability of expression since they are capable of violating privacy rights, and thus both will be assumed to have rights of freedom of expression.

Further, the publishing of private information should be given the right to erasure based on the individual's right to privacy under the relevant EU law.[88] The individual's right to privacy under the RTE and the GDPR can be derived from Article 17(1)(d)-(e).[89] Article 17(1)(d) states that the right of erasure is applicable when "the personal data have been unlawfully processed."[90] Under this definition, published information that has been unlawfully processed can consequently be deemed illegally published. Collecting information by violating an individual's privacy according to any relevant EU law will subsequently be unlawfully processed personal data. Furthermore, Article 17(1)(e) states that "the personal data have to be erased for compliance with a legal obligation in a Union or Member State law to which the controller is subject."[91] This Article gives rise to the right of privacy under EU law and can be understood to require the GDPR RTE to comply with the individual's right to privacy under EU law.

B. Right to Erasure vs. Freedom of Expression

The tensions between Article 8 (right to respect for private and family life) and Article 10 (freedom of expression) are easy to identify, yet difficult to reconcile.[92] To what extent does erasure conflict with Article 10 of the Convention? Article 8 of the Convention states that a public authority shall not interfere with the right to respect for private and family life except when necessary in a democratic society and in accordance with the law. Article 8 also carves out circumstances when a public authority can interfere with the right to respect, including reasons for national security, public safety, the country's economic well-being, crime prevention, health reasons, or "the protection of the rights and freedoms of others."[93] Accordingly, a public authority may interfere with an individual's

[87] *See generally* German Federal Court of Justice, *Liability of Search Engine Operator for Autocomplete Suggestions that Infringe Rights of Privacy -- "Autocomplete" Function*, 8 J. OF INTELL. PROP. L. & PRACTICE 797 (2013).
[88] *See supra* Section II, D.
[89] Regulation (EU) 2016/679, art. 17(1)(d)-(e), 2016 O.J (L 119/1) 43, 44.
[90] *Id*. art. 17(1)(d).
[91] *Id*. art. 17(1)(e).
[92] *See* European Convention on Human Rights, *supra* note 37, at art. 10.
[93] *Id*. sec. I, art. 8.

exercise of the right to respect private and family life in order to explicitly protect freedom of expression.

However, Article 10 of the Convention states that the exercise of the freedoms of expression may be subject to formalities, conditions, restrictions, or penalties, and lists the same reasons for its limitation as Article 8, and adds additional circumstances which include, "the protection of the reputation or rights of others," and "preventing the disclosure of information received in confidence."[94] Accordingly, the Convention has imposed more limitations on the right to freedom of expression than the right to privacy, and has built in privacy protections within Article 10 to ensure that the freedom of expression does not blatantly interfere with individuals' privacy rights.

The court in Google Spain v. AEPD ruled that Google must remove an individual's private information, but did not impose the same ruling on the newspaper that initially published the individual's information.[95] Google removes the information by "delinking" or "unlinking" the newspaper's page from its search results.[96] This permits the removal of information without effectively "erasing" or "forgetting" the information, exposing the inaccurate title of Article 17. Seemingly, freedom of expression concerns may have influenced the court's decision when they decided to limit the removal of information to Google alone, and the court may have intended to strike a balance between erasure and the freedom of expression.[97]

C. Analyzing the Treatment of Data Privacy Cases by EU Courts

Analyzing and assessing the EU's treatment of privacy cases is necessary to suggest an effective solution. While the cases have been decided based on the Directive's RTBF, the ruling will inevitably affect future decisions made under GDPR's RTE. Neither the reasoning nor the outcome of the data privacy cases have been consistent. However, by closely analyzing factors courts deemed important, the recommendation will be able to reconcile the different reasoning approaches taken by the judges and distinguish the cases with differing outcomes. The cases below have been divided into categories based on the nature of the data and the court's reasoning.

---

[94] *Id*. sec I, art. 10.
[95] *See* Case C-131/12, Google Spain v. AEPD, 2014 E.C.R. 317, 21 (May 13, 2014).
[96] *See generally* Jeffrey Toobin, *The Solace of Oblivion: In Europe, the right to be forgotten trumps the Internet*, THE NEW YORKER (Sept. 29, 2014), https://www.newyorker.com/magazine/2014/09/29/solace-oblivion [https://perma.cc/2WL2-LGN2].
[97] *See* Case C-131/12, Google Spain SL v. AEPD, 2014 E.C.R. 317.

1. Considering the Circumstances of the Intrusion

The ECtHR has considered the circumstances and places in which actions take place to decide whether they are in fact, private. In Von Hannover v. Germany, the ECtHR held that there was a violation of Article 8 of the Convention when German magazines published photographs of Princess Caroline engaging in private activities such as horseback riding, shopping, on a bicycle, and spending time with her children.[98] The ECtHR generally concluded that the published photos related to her private life and did not make a contribution to a debate of general interest.[99] While the public figure in this case links to GDPR Article 17(3)(d) and the public interest which is outside the scope of this Note,[100] this case closely deals with the right to privacy in the Convention and the right to respect for private and family life.[101] In Von Hannover v. Germany (no. 2), the courts looked at "the circumstances in which the photos had been taken" as well to make their determination.[102]

Analyzing the likely outcome of this case under common law privacy concepts can highlight similarities and discrepancies of different privacy laws. Under the English common law of confidence, Princess Caroline's pictures would not be protected as there was no implied contract of confidentiality between two parties. Under Prosser's torts, the pictures may be considered private under "intrusion upon seclusion or solitude, or into private affairs."[103] Had Princess Caroline conducted these actions in the public sphere, it is unlikely that her photos would be protected under the right to privacy, and it would have been more likely for the right to freedom of expression and information to prevail in this case.

The ECtHR sometimes takes the role citizens play in society into consideration, and distinguishes between the publication of facts and rumors. In Mosley v. United Kingdom, the plaintiff challenged the publication of a news story by "News of the World" that included embarrassing sexual information regarding his private life and argued for imposing a legal duty to notify him prior to publishing

[98] *See Von Hannover v. Germany*, Eur. Ct. H.R. (2004), https://hudoc.echr.coe.int/eng#{"dmdocnumber":["699729"],"itemid":["001-61853"]}[https://perma.cc/7DB3-GQ5S].
[99] *Id*. at 27. *See also Von Hannover v. Germany (no.2)*, 40660/08 & 6064/08 Eur. Ct. H.R. 39 (2012) (holding that national courts "carefully balanced the right of the publishing companies to freedom of expression against the right of the applicants to respect for their private life").
[100] GDPR, art. 17(3)(d).
[101] European Convention on Human Rights, *supra* note 37, at art. 8.
[102] *Von Hannover v. Germany (no.2)*, 40660/08 & 6064/08 Eur. Ct. H.R. 24 (2012).
[103] Prosser, *supra* note 71, at 389.

the story.[104] The ECtHR found that Article 8 of the convention did not require publishers to notify individuals before they published information about their private lives.[105] Although the case involved an invasion of privacy, the court noted that "there is a distinction to be drawn between reporting facts—even if controversial—capable of contributing to a debate of general public interest in a democratic society, and making tawdry allegations about an individual's private life."[106] This case generated a lot of media,[107] and ultimately presents an example of the limits of the right to privacy.[108] The court in this case was conscious about the chilling effect the right of privacy may have on free speech and refused to allow a notification requirement for the publication of facts.[109] Although the question of this case was not whether the private sexual acts were considered "private," they would likely be considered "private" under both Prosser's torts and the law of confidence.[110]

2. Reasonable Relationship of Proportionality

The ECtHR considers and balances both the right to privacy and the right to freedom of expression when deciding cases, as well as the impact their decisions will have on these separate rights. In Axel Springer v. Germany, albeit not a RTE request, the court refused to provide an actor with an injunction preventing the

[104] *See Mosley v. United Kingdom*, 48009/08 Eur. Ct. H.R. 18 (2011), http://www.5rb.com/wp-content/uploads/2013/10/Mosley-v-UK-ECHR-Application-no-48009_08.pdf [https://perma.cc/D8QC-ZGGH].
[105] *Mosley v. United Kingdom*, 48009/08 Eur. Ct. H.R. 37 (2011); SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017, *supra* note 28, at 258.
[106] *Mosley v. United Kingdom*, 48009/08 Eur. Ct. H.R. 31 (2011); SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017, *supra* note 28, at 258.
[107] *See e.g.*, Max Mosley, *We Need a Law on Prior Notification*, GUARDIAN (Feb. 24, 2010), https://www.theguardian.com/commentisfree/libertycentral/2010/feb/24/privacy-law-prior-notification [https://perma.cc/7QPC-GDQM]; Tom Wells, *Mosley Takes a Proper Spanking*, SUN (May 10, 2011), https://www.thesun.co.uk/archives/news/536321/mosley-takes-a-proper-spanking/ [https://perma.cc/4VSQ-QWRX].
[108] *See generally Case of Mosley v. The United Kingdom*, Global Freedom of Expression, COLUM. UNIV. (last visited Apr. 7, 2018), https://globalfreedomofexpression.columbia.edu/cases/case-mosley-v-united-kingdom/ [https://perma.cc/4YAV-9SHJ].
[109] *Mosley v. United Kingdom*, 48009/08 Eur. Ct. H.R. 774 (2011).
[110] Prosser, *supra* note 71, at 389; *The Common Law Duty of Confidentiality*, UK Department of Health (last visited Apr. 7, 2018), http://webarchive.nationalarchives.gov.uk/+/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_5803173 [https://perma.cc/DV7S-TPWZ].

publication of information regarding his drug-related offense.[111] The court held that "there is no reasonable relationship of proportionality between, on the one hand, the restrictions imposed by the national courts on the applicant company's right to freedom of expression, and on the other hand, the legitimate aim pursued."[112] In the case that convictions are regularly made public, removing information from public access or preventing its publication is only limiting free speech because the individual does not initially have a right to privacy regarding publications of information regarding public safety or national security according to Article 8 of the Convention.[113]

3. The Nature of Publicly Available Information

In some cases, the nature of the private information bears heavier weight in the court decisions, even when the information is already publicly-available. This usually diminishes the chances that the information is characterized as "private." In Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,[114] a publisher published individuals' publicly-available tax-related data.[115] The court held that "extensive publication of personal, publicly-available tax information constituted a violation of Article 8, especially in light of Article 10's protection of a free press."[116] However, this information will not be covered under both the law of confidence nor under Prosser's torts despite its private nature because they were publicly available.

4. Private Information in the Public Sphere

Information in the public domain or that is widely-known is regularly treated differently by the court, even when it is usually considered private. In *Lindqvist*, a woman published extensive information about her work colleagues, including their names, hobbies, family circumstances, phone numbers, and other personal information, such as details regarding a colleague's injury on a webpage,

---

[111] *Axel Springer v. Germany*, 39954/08 Eur. Ct. H.R. 34 (2012), https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2017/10/CASE-OF-AXEL-SPRINGER-AG-v.-GERMANY.pdf [https://perma.cc/B58X-BMPL].
[112] *Id*.
[113] European Convention on Human Rights, *supra* note 37, art. 8.
[114] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, 931/13 Eur. Ct. H.R. 3 (2015), https://lovdata.no/static/EMDN/emd-2013-000931-2.pdf [https://perma.cc/6PM6-EVEC].
[115] *Id*.; SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017, *supra* note 28, at 259.
[116] *Id*.

that could be accessed from her Church's home page.[117] The purpose was charitable, and aimed to enable parishioners to easily obtain information.[118] The woman removed the information once her colleagues voiced their objections. Despite doing so, she was charged with criminal violations of Swedish data protection law.[119] However, the European Court of Justice (ECJ) stated that her activities did not fall within the scope of the Directive and were not a disproportionate violation of the freedom of expression.[120] This case would not be covered under Prosser's torts because this information is likely to be viewed as public facts as a large number of people are aware of the facts surrounding these individuals and the facts are in the public domain. However, parts of this information such as the parishioners' family circumstances and phone numbers and the colleague's injury may be covered under the law of confidence since the information was provided with an expectation that it would remain confidential.

D. The Elements of Erasure

As explained above, both Prosser's privacy torts and the law of confidence can be used to determine whether published material is private and is entitled to the right to erasure. However, solely adhering to these concepts of privacy in the context of publishing private information as freedom of expression and information will limit the concept of privacy, and in some circumstances unnecessarily expand it. However, placing blanket-definitions over the concept of privacy will limit the freedom of expression and information.

Both Prosser's privacy torts and the law of confidence cannot be used to identify private information in this context. Prosser's torts overwhelmingly focus on private information that result in negative consequences. Prosser's first element is covered by Article 8 of the Convention.[121] Further, Prosser's second and third elements may have negative effects on public interest and the freedom of expression, and Prosser's fourth element is now covered by libel, defamation, and intellectual property law.[122] Additionally, the law of confidence protects an overwhelmingly large amount of information by protecting both private and non-

[117] Case C101/01, Lindqvist v. Åklagarkammaren i Jönköping, 2003 E.C.R. I-12971, ¶ 17. http://curia.europa.eu/juris/showPdf.jsf?text=&docid=47672&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=156834.
[118] *Id*.
[119] Laraine Laudati, *Summaries of EU Court Decisions Relating to Data Protection 2000-2015*, OLAF, (Jan. 28, 2016), https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf.
[120] *Id*. at 45.
[121] European Convention on Human Rights, *supra* note 37, at art. 8.
[122] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

private confidential information. This too may have unintended negative impacts on public interest and the freedom of expression and information.

As a result, this Note proposes the elements of erasure (EOE); the elements consider whether there was a reasonable expectation of privacy, whether there was a reasonable expectation of a duty of confidence, how the information was collected, and whether an individual is personally identifiable using the collected information. The EOE is a balancing test that takes into consideration comprehensive factors that should be assessed to determine whether published information is considered private information. If the information is private, a determination should be made on whether it is entitled to the right to erasure (RTE). Otherwise, it would be considered an exercise of the right of freedom of expression and information.

The following balancing test aims to reconcile the aforementioned cases and provide courts with a consistent approach to analyze and determine the sufficiency of RTE requests. The EOE aim to clarify what falls under the right of privacy and is entitled to the RTE when the individual case does not neatly fall under one of the subsections of Article 17(1). However, this balancing test is irrelevant when Article 17(3)(b)-(e) (RTE exceptions) are clearly applicable.[123] Article 17(3)(d) is particularly problematic and is often intertwined with cases that discuss the RTE versus the right of freedom of expression and information. Nonetheless, it is a separate argument outside the scope of this Note, and this Note aims to distinguish freedom of expression cases from public interest cases to the utmost extent possible.

1. Was There a Reasonable Expectation of Privacy?

First, the court must ask whether there was a reasonable expectation of privacy in the case of the information published. Whether the actions were conducted in public and whether they concern private and family life, as outlined in Convention's Article 8, are included within this element. In *P.G. & J.H. v. United Kingdom*, while not directly relevant to the topic, the court stated that a factor that affects Article 8's protection of private life "outside a person's home or private premises" is "a person's reasonable expectations as to privacy."[124] In *Mosley v. United Kingdom*, Mosley was a public individual with a famous name and family

[123] *See* GDPR, *supra* note 2, at art. 17.
[124] P.G. & J.H. v. United Kingdom, 44787/98 Eur. Ct. H.R. (2011); SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017, *supra* note 28, at 258.

history, and could be argued to have a lower expectation of privacy.[125] Additionally, in *Satakunnan*, the court found that an individual has a reasonable expectation of privacy regarding their tax information.[126]

This element must allow for a comprehensive view of the facts. For example, this element would hold that a President does not have a reasonable expectation of privacy regarding their tax-related information based on their public role in society, yet a private individual would have a reasonable expectation of privacy concerning the same information. Moreover, in Von Hannover (no.2), the court stated that the circumstances in which the photos were taken were relevant.[127] Individuals are unlikely to have a reasonable expectation of privacy when they are expressing themselves outwardly in the public sphere that a casual observer would notice. However, a person does not expect that a stranger might be chronicling their exact moves in public, nor does a person expect to be "upskirted" in public. Consequently, an expectation of privacy may still exist in the public sphere, but a comprehensive view of the facts is imperative.

2. Was there a Reasonable Expectation of a Duty of Confidence?

Second, the court must ask whether there was a reasonable expectation of a duty of confidence. This factor stems from the English law of confidence with an added element of reasonableness. Questioning whether a reasonable expectation of this duty exists is necessary because without it, the English common law is overbroad and protects both private and non-private information. Warren and Brandeis initially published their infamous article when cameras became a commodity and capturing faces and everyday scenes was unprecedented.[128] Technology has rapidly developed since then and as a consequence, our expectations of privacy have decreased. The duty of confidence holds where a reasonably prudent person would expect an implied contract of confidentiality taking into consideration general circumstances surrounding the case. Further, identical to the English law, this Note proposes that the three circumstances that allow the disclosure of confidential information should remain unchanged: first, where the individual to whom the information related has consented; second, where

[125] *Max Mosley: Life in the Fast Lane*, BBC (May 10, 2011), http://www.bbc.com/news/uk-13338571.
[126] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 931/13 Eur. Ct. H.R. (2015).
[127] Von Hannover v. Germany No.2, 40660/08 & 6064/08 Eur. Ct. H.R. (2012).
[128] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)., https://www.engineersgarage.com/invention-stories/camera-history

disclosure is in the public interest (which will be left for courts and legislators to define) and third, where there is a legal duty to do so.[129]

This element focuses on the relationships between the parties involved in the transfer of information. For example, in *Mosley v. United Kingdom*, Mosley had a reasonable expectation of a duty of confidence between himself and the other party in his sexual encounter because an individual reasonably expects intimate sexual acts to remain confidential.[130] However, in a case like *Bodil Lindqvist*, a court would probably find that individuals should not have a reasonable expectation of a duty of confidence regarding general information they voluntarily provided about themselves.[131] Yet, the court might find that a reasonable expectation of a duty of confidence exists if one of Lindqvist's work colleagues shared sensitive family circumstances with her, especially if they maintained a close relationship built on trust.

3. How was the Information Collected?

Third, the courts must look at the means used to collect private information, which is increasingly complex and always important given the state of the internet and surrounding technologies. This factor also aims to address issues in *Von Hannover* and paparazzi and tabloids in general, as well as what this Note terms "second-hand publishing." When paparazzi are excessively intrusive and do not respect individuals' private life, home, and correspondence in accordance with the Convention Article 8,[132] then the information is more likely to be labeled as private information. Also, if the information is already in the public sphere or made public by the individual via a blog and a publisher who has access to this information chooses to publish the information second-hand, it is less likely to be considered private information.

This element focuses on the source of the information and the means used to access the information. For example, if the paparazzi were intrusive in obtaining Princess Caroline's pictures in Von Hannover v. Germany, or accessed her home or communications illegally, this would constitute a violation of the right to privacy and find that the information was obtained improperly.[133] However, in *Oy v. Finland*, the tax-related data was already publicly-available, and the publisher only

[129] *See* discussion *supra* Part II.F.3.
[130] *Mosley v. United Kingdom*, 48009/08 Eur. Ct. H.R. 28 (2011).
[131] Case C-101/01, Lindqvist v. Åklagarkammaren i Jönköping, 2003 E.C.R. I-12971.
[132] European Convention on Human Rights, art. 8.
[133] Von Hannover v. Germany, 59320/00 Eur. Ct. H.R. 34-35 (2004).

engaged in "second-hand publishing."[134] Overall, the information may still be considered private under the first EOE because there is a reasonable expectation of privacy associated with tax-related data due to its sensitive nature, and the publisher may have increased access to the information or harmed the individual by aggregating the data in one location. However, under the third EOE, the tax-related data was not obtained through intrusion or illegal methods.

4. Is an Individual Personally Identifiable Using the Disclosed Information?

Fourth, the court must determine whether an individual is personally identifiable using the disclosed information. In some cases, such as an autobiography that details the life of another person whose identity is not crucial for public interest reasons or otherwise, or a news story about a rare disease that does not require divulging personal identities, and so on, private information should not act as a hindrance to the disclosure of the information. However, the identity of the individual should consistently be protected when private information that could be deemed otherwise useful and should not be restricted is divulged. In these cases, information should be disclosed provided that it is not traceable to the individual related to the data. Professor Daniel Solove states that the use of pseudonyms or initials are a workable compromise in such contexts and states that, "[j]ournalists generally do not include the names of rape victims or whistleblowers in their stories. On television, the media sometimes obscures the faces of particular people in video footage. With minimal effort, the media can report stories and also protect privacy."[135]

This element aims to ensure that the freedom of expression is not stifled due to privacy concerns. For example, in Bodil Lindqvist, merely removing an individual's name is insufficient because the individuals remain personally identifiable through their home addresses, telephone numbers, and other identifying information provided on the site.[136] However, if a publisher blurred out the faces and obscured any identifying elements connected to individuals pictured around a crime scene, the individuals will likely no longer be personally identifiable. These actions can be sufficient to avoid interfering with an individual's right to privacy.

[134] Oy v. Finland, 931/13 Eur. Ct. H.R. 52, 55-56 (2015).
[135] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 Duke L.J. 967, 1021 (2003).
[136] Lindqvist, *supra* note 130.

E. Applying the Elements of Erasure to Google Spain v. AEPD

To illustrate the application of the EOE factors, this Note will apply them to Google Spain v. AEPD. First, was there a reasonable expectation of privacy? One can argue that there was no reasonable expectation of privacy because real estate auctions are often published in the media and the real estate auction was a public affair. However, in this particular case, the announcement was published, mentioned the individual's name, and detailed that the real estate auction was conducted for the recovery of social-security debts which could be argued to exceed the information needed to publicize a real estate auction. Additionally, if the court were to find that most auction sellers are anonymous, this would strengthen the individual's expectation of privacy. Second, was there a reasonable expectation of a duty of confidence? This factor is not prevalent in this case as we do not have enough information regarding the people the information was shared with. Third, how was the information collected? Google Spain's algorithm linked to La Vanguardia newspaper. Consequently, the information was collected appropriately, meaning that this factor does not weigh in favor of the RTE. Fourth, is the individual personally identifiable using the disclosed information? In this case, the individual was clearly personally identifiable; his name, Costeja Gonzalez, alongside information regarding his debts were publicized. The fourth factor strongly weighs in favor of the RTE in this case, especially since publicizing his personal information is not central to the real estate auction purposes. Overall, the deciding factor may hinge on whether the court finds that there was a reasonable expectation to privacy. Consequently, using the EOE, a court will likely find that Mr. Gonzalez is entitled to the RTE.

This case lies on the fringes of the right to privacy, explaining the highly controversial ruling of the case. Nonetheless, the EOE balancing test provides a consistent method to evaluate RTE requests by distilling haphazardly-decided privacy cases into four central elements.

CONCLUSION

In conclusion, the RTE supports the erasure of published personal data that has been unlawfully processed. Under EU law, an explicit right to privacy exists under GDPR Article 17. To adequately determine whether individual cases are entitled to erasure due to a privacy violation, the EOE present factors that enable a court to comprehensively evaluate privacy rights in relation to the right to freedom of expression in this particular context. Additional research should be conducted to further distinguish the RTE's treatment of traditional controllers (e.g., online

magazines) from untraditional controllers (e.g., search engines). This can be done once the GDPR is enforced and courts issue rulings that provide an indication of how, if at all, different controllers should be distinguished under the law in this context. Nevertheless, the EOE balancing test equips the courts with a straightforward method to evaluate and protect the right to privacy without unnecessarily limiting the freedom of expression and information.

APPENDIX A

GDPR Article 17 "Right to erasure ('right to be forgotten')"[137]

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based according to point (a) or Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union of Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controlled is subject or for the performance of a task carried out in the public interest of in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance

[137] *See* GDPR, *supra* note 2, at art. 17.

with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defense of legal claims.