Where Next for the Right to Delete: Stepping Out of the Shadow of the Right to be Forgotten

Alan Harrison*

TABLE OF CONTENTS

* J.D., May 2023, National Security and Cybersecurity Concentration, The George Washington University Law School, and Research Assistant for Professors Daniel J. Solove, John Marshall Harlan Research Professor of Law, and Laura A. Dickinson, Oswald Symister Colclough Research Professor of Law. M.P.S., May 2019, Legislative Affairs, Graduate School of Political Management, George Washington University. B.A., May 2016, Economics and Political Science, George Washington University. I have immense gratitude towards the staff and Editorial Board members of the FCLJ for their publication support and comments, and to all those who supported this note's development, including: Meredith Rose and Natasha Nerenberg, my Journal Adjunct Advisor and Notes editor; Professor Solove; Stacey Gray and Amie Stepanovich, Senior Director for U.S Policy and Vice President for U.S. Policy at the Future of Privacy Forum for their early encouragement of this topic; and lastly to my family for all of their encouragement.

I. INTRODUCTION

In 2018, California enacted the California Consumer Privacy Act ("CCPA"), granting California consumers a number of rights against data-holders to give them "more control over [their] personal data."[1] One of these rights is the right to request that a business or organization delete one's personal information.[2] Concerns linger regarding how to implement the statute's right to delete ("RTD"); of particular concern are the numerous exceptions to the right.[3] Other states have enacted their own state privacy statutes with Virginia, Colorado, and Utah all including the RTD with similar exemptions within their state privacy bills.[4]

While the RTD has been gaining traction in current and pending privacy bills in the United States, there has been little focus on its scope, effect, and technical implementation. This Note delves into the RTD with the intent of analyzing its immediate limitations that prevent the right from realizing its full effectiveness within a consumer privacy regime of rights.

The first step in analyzing the RTD in its current form is to clearly define the right. Imbedded with that step, however, is an antecedent step of distinguishing the RTD from the right to be forgotten ("RTBF"). The RTD (which is the European functional equivalent to the right of "erasure") is often

1. *California Consumer Privacy Act (CCPA)*, OFF. OF ATT'Y GEN., STATE OF CA. DEP'T OF JUSTICE, https://oag.ca.gov/privacy/ccpa [https://perma.cc/6M5T-CY6Q] (last visited Mar. 27, 2022).

2. *Id.*

3. Yoni Bard & Scott Bloomberg, *CCPA: The (Qualified) Right to Deletion*, JD SUPRA (July 25, 2019), https://www.jdsupra.com/legalnews/ccpa-the-qualified-right-to-deletion-40847 [https://perma.cc/37UQ-MV88]; *see also* Ilia Sotnikov, *Six Top Concerns of CCPA Compliance*, SECURITYINFOWATCH.COM (Apr. 29, 2019), https://www.securityinfowatch.com/cybersecurity/information-security/article/21078368/six-top-concerns-of-ccpa-compliance [https://perma.cc/L45U-SLH9] (describing numerous first-glance issues of the CCPA as proposed, including a "list of exceptions [to the right to delete] so broad that companies can come up with legitimate excuses not to delete data at all.").

4. *See* Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-571-581 (West, 2022), Colorado Privacy Act, COLO. REV. STAT. ANN. §§ 6.1.1301-1313 (West, 2023), S.B. 1392, 161st Gen. Assemb., 1st Spec. Sess. (Va. 2021) (enacted, Consumer Data Protection Act); S.B. 21-190, 73rd Gen. Assemb., Reg. Sess. (Colo. 2021) (enacted, Colorado Privacy Act); S.B. 227, 2022 Leg., Gen. Sess. (Utah 2022) (enacted, Utah Consumer Privacy Act); Jake Holland, *Utah Privacy Bill Signed, Making Fourth State with Such a Law*, BLOOMBERG LAW (Mar. 24, 2022, 2:56 PM) https://news.bloomberglaw.com/privacy-and-data-security/utah-privacy-bill-signed-marking-fourth-state-with-such-a-law [https://perma.cc/BY3X-SJR6].

either conflated with the RTBF or analyzed in relation to the RTBF.[5] While they share similar characteristics, in part because of the technical nature of implementing each right, they are clearly distinct rights with different purposes.

The second step for this Note—once the RTD has been clearly distinguished from the RTBF—is to address the most critical issues that will help ensure the effectiveness and full scope of the RTD. The most significant issue is the lack of standardization in the definition and the technical process of "deletion" once a consumer submits a request to an entity to delete their personal data. This lack of consistency stems from the variety of state data disposal laws (which will control in each state that passes a state privacy law) and the absence of a standard definition of deletion within privacy bills that aligns with technical definitions of deletion. Almost as critical is the issue of exemptions to consumer requests to delete personal data when an entity deidentifies (or pseudonymizes) personal data in lieu of deletion. This Note suggests that this exemption grants a false sense of security to the consumer and potentially defeats the purpose of the RTD due to recent leaps forward in reidentification science. Thus, consumer deletion requests that are exempted in this way defeat the purpose of the right, which is to shift the balance of control over privacy towards consumers and away from data holders.

II. BACKGROUND

This part of the Note will discuss the scope and contours of (1) the RTBF's European origin and its unsuccessful story in the United States; and (2) the RTD as established within the CCPA and subsequent U.S. state privacy bills. A contextual approach is necessary to distinguish the RTD from the RTBF and to map the similarities and differences between them. By distinguishing the two rights, it becomes clear that the act of deletion serves a different purpose within each right. Whereas the RTBF views the act of

5. *E.g.,* Yaki Faitelson, *Why 'Right to Delete' Should Be On Your It Agenda Now*, FORBES: TECH COUNCIL (Oct. 22, 2018, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/10/22/why-right-to-delete-should-be-on-your-it-agenda-now/?sh=5f7382a31b7f [https://perma.cc/FX3Y-5MXJ] ("In 2020, the [California Consumer Privacy Act] will give consumers some of the same rights as the [European Union's General Data Protection Regulation], including the right to delete personal information on demand."). *But see* Regulation 2016/679, of the European Parliament and of the Council of 27 Apr. 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), art. 17, 2016 O.J. (L 119) 43-44 [hereinafter GDPR] (providing for the "Right to erasure ('right to be forgotten')"). The GDPR conflates the two rights by including the RTBF within the title of the right to erasure, which gives a consumer "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay." *Id.* at 43. With each repetition of the privacy rights established by the GDPR, this conflation of two distinct rights has grown. *See, e.g.*, *Right to Erasure*, INFO. COMM'R'S OFF. (UK), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ [https://perma.cc/JQ6F-KZBM] (last visited Apr. 11, 2022) ("The UK GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as the 'right to be forgotten.'").

deletion as a mechanism to achieve the substantive goal of digitally forgetting data (akin to human memory's natural retention limitation), the RTD views the act of deletion as the goal itself in order to empower greater consumer control over one's personal data.

A. The Right to Be Forgotten

1. The European Origins of the Right to Be Forgotten

The ambiguity of distinguishing between the RTBF and the RTD is in part due to terminology used to describe the evolution of the RTBF prior to (and during) the digital age. As recently as 2010, a European Commission Communication described the RTBF as "the right of individuals to have their data no longer processed *and deleted* when they are no longer needed for legitimate purposes."[6] The RTBF addresses the indefinite retention of digital information to theoretically grant a "dimension of oblivion, granting individuals a 'fresh start.'"[7] A natural tool to redress this harm is data deletion, whether cyclical and automatic or on an ad hoc and individual basis. The animating policy argument is that in the digital age, society must actively delete (and thus forget) information in order to mitigate the societal consequences created by external memory, which makes it cheaper to remember than to forget.[8] This need, advocates argue, has been amplified with trends such as "smart" devices extending from TVs, to doorbells, to lightbulbs that can integrate into Google Home-, Siri-, or Alexa-enabled networks.[9] To address this data permanence and restore digital memory to levels comparable to pre-digital society levels, digital storage devices (e.g., cameras, cellular devices, or computers) "should automatically delete information that has reached [a designated] expiration date."[10]

The RTBF itself can be traced to French law, which recognizes *le droit à l'oubli* (the "right of oblivion," which allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration),[11] as well as the Italian *diritto all'oblio* (which has been described as "the right to silence on past events in life that

6. European Commission Communication COM/2010/0609, A Comprehensive Approach on Personal Data Protection in the European Union (Nov. 4, 2010) (emphasis added).

7. Aurelia Tamò & Damian George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5 J. INTELL. PROP., INFO. TECH. & E-COM. L. 71, 73 para 17 (2014).

8. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 169 (2011).

9. Adam Levin, *Selling Privacy: The Next Big Thing for Entrepreneurs*, INC. (Dec. 5, 2019), https://www.inc.com/adam-levin/selling-privacy-next-big-thing-for-entrepreneurs.html [https://perma.cc/CF9H-X4LS].

10. Stuart Jefferies, *Why We Must Remember to Delete – and Forget – in the Digital Age*, GUARDIAN (June 30, 2011, 3:30 PM) https://www.theguardian.com/technology/2011/jun/30/remember-delete-forget-digital-age [https://perma.cc/L8NG-BJQX].

11. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012).

are no longer occurring").[12] Similar rights developed in the jurisprudence of other European countries over the 20th century. In the United Kingdom, for example, the Rehabilitation of Offenders Act of 1974 reflects a principle of this right in the rehabilitation of past offenders.[13]

The RTBF, while not explicitly stated, can also be found by implication in various German legislation and jurisprudence. In 2013, German courts found that the RTBF, as an extension of the modern right to data protection under the Data Protection Directive of 1995, could be sourced not only from the idea of privacy, but also the German constitutional right to self-determination.[14] Specifically, the German Constitution guarantees that "every person shall have the right to free development of his personality."[15] Prior to the Data Protection Directive, in 1984, the Federal Labor Court linked the constitutional right of self-determination to the conventional European RTBF.[16] The court addressed whether a person had a "right to erasure of data that the data subject had disclosed himself" and held that a "job applicant's right to informational self-determination would be violated if a company who denied the applicant kept his or her data indeterminately."[17] The Federal Labour Court's ruling built on the decision in "*Lebach I*," where the German Federal Constitutional Court in 1973 reviewed a challenge by a murder convict against a television station for a documentary production that allegedly impinged the plaintiff's rights of personality and self-determination.[18] The court was asked to balance two competing constitutional rights: (1) the "freedom of the media under Article 5 of the Basic Law," and (2) the "personality rights of the convicted criminal under Article 2."[19] In *Lebach I*, the court held the encroachment of freedom of information "should not go any further than required to satisfy what was necessary to serve the public interest," opining that reports of events long since passed have less public interest if they pose new disproportional risks and "endanger[] the social rehabilitation of the criminal who has" a conviction.[20]

In 1995, the European Council passed Directive 95/46/EC (the "Directive") regarding the "protection of individuals[']… processing of

12. Giorgio Pino, *The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights*, *in* THE HARMONISATION OF EUROPEAN PRIVATE LAW 225, 236 (Mark Van Hoecke & François Ost eds., 2000).

13. Rehabilitation of Offenders Act, (1974) c. 53, pmbl. (Eng.) ("An Act to rehabilitate offenders who have not been reconvicted of any serious offence for periods of years, to penalise the unauthorised disclosure of their previous convictions, to amend the law of defamation, and for purposes connected therewith.").

14. Claudia Kodde, *Germany's 'Right to Be Forgotten' - Between the Freedom of Expression and the Right to Informational Self-Determination*, 30 INT'L REV. L., COMPUTS. & TECH. 17, 19 (2016).

15. GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [CONSTITUTION] May 8, 1949, art. 2, § 1 (Ger.).

16. Kodde, *supra* note 14, at 27.

17. *Id.*

18. *Id.* at 26.

19. Nicole Jacoby, *Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States*, 35 GA. J. INT'L & COMPAR. L. 433, 463 (2007).

20. Kodde, *supra* note 14, at 26.

personal data."[21] The Directive did not expressly include the right to be forgotten. Nonetheless, in 2014, the Spanish High Court asked the Court of Justice of the European Union ("CJEU") to determine "the scope of the right of erasure and/or the right to object, in relation to the '*derecho al olvido*' ("RTBF")" under the Directive.[22] In *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos* (*AEPD*) *and Mario Costeja González* (hereafter "*Google Spain*"), the CJEU considered whether the Directive created a right of erasure of true (but prejudicial) information that the subject "wishes . . . to be 'forgotten' after a certain time."[23] In the original complaint, Mr. González argued that under the Directive, "fundamental rights to the protection of those data and to privacy—which encompass the 'RTBF'—override the legitimate interests of the operator of the search engine and the general interest in freedom of information."[24] The CJEU found that the Directive's fundamental privacy rights included the right of a private citizen to request that his or her private name be removed from lists of "links to web pages published lawfully by third parties and containing true information relating to him."[25] The CJEU further found that this right overrides "the economic interest of the operator of the search engine [and] also the interest of the general public in finding that information upon a search relating to the data subject's name."[26]

The case has been studied by commentators both broadly and narrowly, and it illustrates the technical and legal ambiguity of key terms such as: forget, erasure, de-list, and delete.[27] On a narrow interpretative scale, *Google Spain's* holding was limited to processor obligations "to remove links to web pages" or to de-list.[28] Narrow-holding interpreters would state that the court explicitly did not find "that a 'RTBF' exists" and that it would be "misleading" to read in a RTBF outside of situations where "the data processing is incompatible with the Directive."[29] For those advocating a broad interpretation, *Google Spain* was a "ground-breaking" opening salvo. [30] In this interpretation, the court's decision to recognize an extensive RTBF that includes the "deletion or erasure of information that a data subject has disclosed passively" was "hardly surprising."[31]

---

21. Directive 95/46, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

22. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶ 20 (May 13, 2014).

23. *Id.* at ¶ 89.

24. *Id.* at ¶ 91.

25. *Id.* at ¶ 89.

26. *Id.* at ¶ 97.

27. *See, e.g.*, Orla Lynskey, *Control over Personal Data in a Digital Age:* Google Spain v. AEPD and Mano Costeja Gonzales, 78 MOD. L. REV. 522, (2015) (for a narrow interpretation); Amy Lai, *The Right to Be Forgotten and What the Laws Should/Can/Will Be: Comparing the United States and Canada*, 6 GLOB. J. COMPAR. L. 77, (2017).

28. Lynskey, *supra* note 27, at 522.

29. *Id.* at 528.

30. Lai, *supra* note 27, at 78.

31. *Id.* at 84, 80.

Even parties to the case characterized the holding differently in the aftermath. For instance, the European Commission's fact sheet about the *Google Spain* case described the Court's ruling as "[o]n the RTBF,"[32] while citing Article 17 (the right to erasure) and detailing the scope of a "request for erasure" as balanced against freedom of expression.[33] In contrast, Google's legal help support page refers to the RTBF as an obligation on processors to "delist certain results for queries" with no mention of obligations to adhere to data erasure requests,[34] while Google's current Transparency Report references the CJEU 2014 ruling without ever using the words "erasure" or "forget."[35] Both sources in unison undermine the clarity of the case's true holding and obfuscates the differences between the RTBF and the right to erasure (the right to delete in the United States).

2. A Rough Landing: The Right to be Forgotten in the United States

Two American cases, both contemporaries of *Google Spain*, demonstrate the uphill battle that litigants seeking to apply the RTBF face in the United States. First, in *Garcia v. Google*, actress Garcia brought a copyright action against YouTube's parent company, Google.[36] Garcia had responded to a casting call and read two lines of script; her voice was later over-dubbed with new lines and incorporated without her knowledge into an entirely new "anti-Islam polemic renamed *The Innocence of Muslims*."[37] A cleric subsequently issued a religious decree against those involved in the polemic.[38] Garcia, in fear for her safety, sought to have *The Innocence of Muslims* removed from YouTube or, in the alternative, have her lines cut from the footage.[39] To do so, she sought an injunction under a copyright theory of harm.[40] On review of a temporary injunction previously granted by a Ninth Circuit panel, the Ninth Circuit, sitting *en banc*, struck down the copyright-based injunction, noting that "[p]rivacy laws, not copyright, may offer remedies" tailored to Garcia's personal and reputation harms.[41] However, the *en banc* court declined to offer a "substantive view" of such an application of

32. EURO. COMM'N, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C-131/12) 1 (2014), https://web.archive.org/web/20140708142544/http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/J5LC-K3DC].

33. *Id.* at 4.

34. *Right to Be Forgotten Overview*, GOOGLE LEGAL HELP, https://support.google.com/legal/answer/10769224 [https://perma.cc/SPA4-E339] (last visited Jan. 26, 2022).

35. *Request to Delist Content Under European Privacy Law*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/eu-privacy/overview [https://perma.cc/N78B-Z3B6] (last visited Jan. 26, 2022).

36. Garcia v. Google, Inc., 786 F.3d 733, 738 (9th Cir. 2015) (en banc).

37. *Id.* at 737.

38. *Id.* at 738.

39. *Id.* at 738-39.

40. *Id.* at 745.

41. *Id.*

privacy law.[42] Further, the court noted that while "Garcia would like to have her connection to the film forgotten and stripped from YouTube," the RTBF, "although recently affirmed by the Court of Justice for the European Union, is not recognized in the United States."[43]

Second, in *Martin v. Hearst Corp*, an individual in a defamation and erasure case sought to have an article that reported on her arrest removed from a publication's website.[44] The State of Connecticut had previously dropped the charges under a *nolle prosequi* agreement, and the "arrest records were erased pursuant to [Connecticut's] Erasure Statute."[45] The individual argued that continued publication of the article was "false and defamatory" because "by the Erasure Statute, she was 'deemed to have never been arrested . . . with respect to the proceedings so erased.'"[46] In denying the cause of action, the Second Circuit interpreted the state erasure statute to establish only a "legal fiction . . . [that] bars the government from relying on the defendant's erased police, court, or prosecution records"; moreover, the presence of the erasure statute within the State's criminal code, as opposed to the civil code, demonstrated the legislature's intent for the statute not "to provide a basis for defamation suits."[47] As "there [was no] dispute that the articles published . . . accurately reported" the arrest, the "various publication-related tort claims necessarily fail[ed]" as a matter of law.[48]

A prevailing criticism against an expanded RTBF in the United States is its potential to disrupt or even harm journalistic endeavors, free speech, and the preservation of records.[49] An empowered RTBF could grant both the "right to suppress unpleasant lies which are publicly told" and may be "extended to unpleasant truths" told about individuals while those individuals are still alive.[50] Further, this disruption to online speech and records can limit natural online discourse.[51] Such criticisms have heightened energy in the United States due to the strong First Amendment protections that some argue are incompatible with the RTBF, while others argue that compatibility is

42. *Garcia*, 786 F.3d at 745.
43. *Id.*
44. Martin v. Hearst Corp., 777 F.3d 546, 548 (2d Cir. 2015).
45. *Id.* at 549.
46. *Id.*
47. *Id.* at 550.
48. *Id.* at 552.
49. *See* David Mitchell, *The Right to Be Forgotten Will Turn the Internet into a Work of Fiction*, GUARDIAN (July 5, 2014, 7:05 PM), https://www.theguardian.com/commentisfree/2014/jul/06/right-to-be-forgotten-internet-work-of-fiction-david-mitchell-eu-google [https://perma.cc/DXQ2-KKK2] (suggesting that the right to be forgotten could undermine the Internet's value to leave for future historians "millions of searchable written sources" for posterity); *see also* James L. Gattuso, *Europe's Latest Export: Internet Censorship*, WALL ST. J. (Aug. 11, 2015, 6:50 PM), http://www.wsj.com/articles/europes-latest-export-internet-censorship-1439333404 [https://perma.cc/D6ZJ-SNKJ].
50. Mitchell, s*upra* note 49.
51. Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. POL'Y 91, 106-08 (2013).

clearly possible.[52] The First Amendment protects freedom of both speech and the press;[53] reflecting the inter-relatedness of both, the media is presumed to have unabridged access to "cover the truth and report it" about "government and public affairs [and] the truth about people."[54] While it is understandable that individuals might wish to be judged on current events rather than past events, in a "free speech regime," external views of a person "should primarily be molded by [readers'] own judgments"[55]—a dynamic potentially at risk when a person can use the RTBF to "keep them in the dark."[56]

However, recent literature has argued that it is possible to accommodate both freedom of speech and the RTBF in the United States. First, there is not an absolute tension between the RTBF and the First Amendment since American law has incorporated elements of the revisability principle—"the opportunity to revise one's beliefs and identity"—and placed it "at the very core of the reason we protect the freedom of expression."[57] Second, "[t]he media portray[al of the] conflict as a clash of two individual rights—the right to be forgotten or, more generally, the right to privacy versus the freedom of speech,"—is flawed.[58] Such an account "masks a far more diverse set of

52. *E.g.,* Farhad Manjoo, *'Right to Be Forgotten' Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html [https://perma.cc/CF85-RVQW] (covering divergent views of the First Amendment's implication on the adoption of the RTBF). An opponent of the RTBF argued that "altering the historical record or making information that was lawfully public no longer accessible to people" is challenging to "square [] with a fundamental right to access to information." *Id.* An advocate of the RTBF countered that "there were ways to limit access to private information that would not conflict with free speech," citing existing processes for the "global removal of some identifiable private information, like bank account numbers, social security numbers and sexually explicit images uploaded without the subject's consent." *Id.*

53. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press . . . .").

54. David A. Anderson, *The Failure of American Privacy Law*, *in* 4 PROTECTING PRIVACY: THE CLIFFORD CHANCE LECTURES 139, 140 (Basil S. Markesinis ed.,1999).

55. Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1093 (2000).

56. *Id.*

57. Andrew Tutt, *The Revisability Principle*, 66 HASTINGS L.J. 1113, 1120 (2015). The "revisability principle" can also be found in the American traditions and values pioneers who sought second chances and reinvention. *See* Meg Leta Ambrose & Jef Ausloos, *The Right to Be Forgotten Across the Pond*, 3 J. INFO. POL'Y' 1, 8 (2013) ("A long history of 'going West' has resulted in appreciation for loosening the shackles of one's past. Reputation is actively protected through mechanisms like defamation and the privacy torts of false light, public disclosure of private facts, intrusion upon seclusion, and misappropriation. Information flow is controlled through legal mechanisms like intellectual property laws and non-disclosure agreements."); *see also* Richard J. Peltz-Steele, *The 'Right to Be Forgotten' Online Is Really a Right to Be Forgiven*, WASH. POST. (Nov. 21, 2014), https://www.washingtonpost.com/opinions/the-right-to-be-forgotten-online-is-really-a-right-to-be-forgiven/2014/11/21/2801845c-669a-11e4-9fdc-d43b053ecb4d_story.html [https://perma.cc/7JFM-YF9T] (describing the RTBF as "really a right to be forgiven; a right to be redeemed; or a right to change, to reinvent and to define the self-anew," and stating that "there could be nothing more American than a second chance in a new world").

58. Edward Lee, *The Right to Be Forgotten v. Free Speech*, 12 I/S: J.L. & POL'Y FOR INFO. SOC'Y 85, 86 (2015).

responses countries can adopt in trying to reconcile the potential conflict."[59] For instance, "the First Amendment is no bar to voluntary industry practices (such as movie ratings and rape shield policies to protect the identities of rape victims)."[60] Further, in countries that have not recognized the RTBF as a matter of law, private companies, such as Google, could recognize the right "in their policies, practices, or technological design."[61]

B. The Right to Delete

1. The Right to Delete as Discussed Before the California Consumer Privacy Act

The technical interchangeability of words such as "erasure" and "delete," as well as the ambiguity surrounding the RTBF during its development, makes mapping the origin of the modern right a challenge. The concept of a "right to delete" has been previously articulated as an implied Fourth Amendment privacy right in the context of a remedy against digital mapping.[62] The right can be viewed as a remedy from a property rights lens: "[i]f imaging is neither search nor seizure, [then] law enforcement agents would have the incentive to image every hard drive they could find" without fear of a Fourth Amendment violation.[63] Advocates of this privacy interest view the Fourth Amendment as "broad enough to protect [a] 'right to destroy' or, in a computer context, [a RTD]" to mitigate the Fourth Amendment evasion of digital copying where the original "physical" property has not be dispossessed.[64]

The RTD as an alternative to the RTBF in the United States could shift the focus away from broad objectives, such as societal forgetfulness and oblivion and towards the idea of personal control over one's data. This removes some tensions with other liberty interests such as freedom of the press. One proposed RTD framework includes four categories of exceptions to an otherwise absolute right to delete: "conflicts with freedoms of speech and of the press; interactions with the right to contract; records associated with multiple individuals; and situations where deletion is impossible, infeasible, or socially harmful."[65] The RTD would further the overachieving privacy regime centered around consumer control and move away from a focus on consumer protection reflected in privacy regulatory elements, such as the minimization principle, which requires a data processor to "delete

59. *Id.*
60. *Id.* at 87.
61. *Id.* at 103.
62. Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10, 11 (2005).
63. *Id.* at 13.
64. *See id.* at 14.
65. Chris Conley, *The Right to Delete*, AAAI SPRING SYMPOSIUM: INTELLIGENT INFORMATION PRIVACY MANAGEMENT 53, 54 (2010), https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482 [https://perma.cc/GH94-BUAU].

unwanted information."[66] Principles such as minimization in support of a RTD help to shift the balance from data holders to data subjects and consumers. Rules providing "practical ways for users to access, modify, and/or delete their data," create a "feel[ing of being] in control," and such "[c]ontrol brings trust" between all involved parties.[67]

2. The Right to Delete as Shaped by the California Consumer Privacy Act

In 2018, California passed a comprehensive state general privacy law.[68] The CCPA provisioned a number of new consumer rights that reflected frameworks for privacy control mechanisms, such as rights of access, correction/modification, and the right (or privacy mechanism) of deletion. The statute gives consumers "the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[69] The CCPA attaches several obligations on businesses that collect consumer data. First, a business must disclose "the consumer's rights to request the deletion of the consumer's personal information."[70] Second, the businesses shall "reasonably verify" that a request to delete comes from a person authorized to make such a request.[71] Upon receipt of a verified request, the company "shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records."[72] While the verification step is arguably a procedural exemption, the CCPA also established a number of specific exemptions limiting the reach of a verified deletion request. For example, the CCPA would limit reach when execution would: impact certain business activities, such as detection of security incidents or activities "within the context of a business' ongoing business relationship with the consumer"; impair "[e]ngage[ment] in public or peer-reviewed scientific, historical, or statistical research in the public interest"; or would prevent a business from "comply[ing] with a legal obligation."[73]

The definition of "personal data" and the activity qualifier "collected from the consumer" limits the scope on the CCPA's consumer right of deletion. While the CCPA provides a broad list of data types that are included in the definition of personal data—from consumer identifiers to biometric

66. EU AGENCY FOR CYBERSECURITY (ENISA), PRIVACY BY DESIGN IN BIG DATA: AN OVERVIEW OF PRIVACY ENHANCING TECHNOLOGIES IN THE ERA OF BIG DATA ANALYTICS 26 (2015), https://www.enisa.europa.eu/publications/big-data-protection/@@download/fullReport [https://perma.cc/8VYR-6KEY].

67. *Id.* at 19-20.

68. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/4A8N-BZHS].

69. CAL. CIV. CODE § 1798.105(a) (West 2020).

70. CIV. § 1798.105(b).

71. CIV. § 1798.140(y).

72. CIV. § 1798.105(c).

73. CIV. § 1798.105(d)(1)-(9).

information and internet activity[74]—it also excludes a broad category of data, namely publicly available information ("PAI").[75] Lastly, the RTD is inapplicable against certain sectorial institutions or institutions that collect certain categories of data such as medical/health information,[76] consumer reporting information,[77] or financial information.[78]

In 2021, Virginia passed its state-wide general privacy act, the Virginia Consumer Data Protection Act ("VCDPA"),[79] followed soon after by the Colorado Privacy Act ("CPA").[80] While the VCDPA and CPA are not identical to the CCPA, all three share broad structural similarities such as the creation of various consumer rights, obligations on data-holders (processors and/or controllers), and technical privacy control mechanisms.[81] All three statutes include a consumer RTD.[82] The VCDPA grants a consumer, or other authorized party, the right to "delete personal data provided by or obtained about the consumer."[83] The VCDPA grants controllers the same procedural exemption to comply with a request only if a controller can "authenticate the request using commercially reasonable efforts."[84] The VCDPA excludes from the definition of personal data "de-identified data or publicly available information."[85]

The CPA provides consumers "the [RTD] personal data concerning the consumer."[86] Mirroring the VCDPA, the CPA provides that controllers are "not required to comply with a request" if they are "unable to authenticate the request using commercially reasonable efforts, in which case the controller may request the provision of additional information reasonably necessary to authenticate the request."[87] The CPA defines personal data as "information

74. CIV. § 1798.140(o)(1).

75. CIV. § 1798.140(o)(2). In 2020, the California Privacy Rights Act (CPRA) amended the definition to also exclude consumer information that "is deidentified or aggregate consumer information." CIV. § 1798.140(o)(3).

76. CIV. § 1798.145(c)(1).

77. CIV. § 1798.145(d).

78. CIV. § 1798.145(e).

79. Christopher Escobedo Hart & Colin Zick, *Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection*, JD SUPRA (July 7, 2021), https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636/ [https://perma.cc/SRA5-VHHM]. For a comparison of each state act's right to delete, see Glenn A. Brown, *Consumers' "Right to Delete" Under US State Privacy Laws*, SQUIRE PATTON BOGGS (Mar. 3, 2021), https://www.consumerprivacyworld.com/2021/03/consumers-right-to-delete-under-us-state-privacy-laws/ [https://perma.cc/JHJ5-J4GA].

80. Hannah Schaller et al., *Colorado Enacts New Consumer Privacy Law*, ZWILLGEN (Aug. 3, 2021) https://www.zwillgen.com/privacy/colorado-privacy-act/ [https://perma.cc/MDJ8-NHVT].

81. For a more in-depth comparative analysis of the three acts, see Cathy Cosgrove & Sarah Rippy, *Comparison of Comprehensive Data Privacy Laws in Virginia, California and Colorado*, INT'L ASSOC. PRIV. PROFS. (July 8, 2021), https://iapp.org/resources/article/comparison-comprehensive-data-privacy-laws-virginia-california-colorado/ [https://perma.cc/N8BZ-54YW].

82. *Id.*

83. VA. CODE ANN. § 59.1-577(A)(3) (West 2021).

84. § 59.1-577(B)(4).

85. § 59.1-575.

86. COLO. REV. STAT. ANN. § 6-1-1306(1)(d) (West 2021).

87. § 6-1-1306(2)(d).

that is linked or reasonably linkable to an identified or identifiable individual" and "does not include de-identified data or publicly available information."[88]

C. *Contrasting the Right to be Forgotten and the Right to Delete*

Both the RTBF and the RTD are concerned with the "protect[ion of] privacy and self-determination interests in the context of permanent memory."[89] But, as an alternative to the RTBF's broad automatic deletion over time approach, the RTD provides consumers the ability to delete "certain records from any permanent repository."[90] Thus, the RTD would grant persons more individualized "control over personal records" than the RTBF would.[91]

The RTBF focuses on addressing the digital retention of information in a new age, the consequences of which affect an individual's rights to privacy and self-autonomy; deletion is a means to an end only, and it is not the focus of the right. The RTD addresses different policy goals, and while the adoption of a RTBF in the United States might overlap with those goals, it would not necessarily further the objectives of the RTD. It is notable that recent state privacy laws include the RTD, while the older RTBF has struggled to gain minimal traction and adoption within the United States, despite the two rights' adjacent policy aims.

For the purposes of this discussion, this Note proposes that there are four salient differences between the RTBF and RTD: (1) the core power each legal right seeks to bestow on individuals; (2) the type of data targeted; (3) the relationship targeted; and (4) the technical implementation of each right.

First, while a RTBF grants the power of anonymity over time, the RTD is focused on empowering data objects with some degree of control over their personal data with respect to the data itself and its holders. "Control" means "to direct" or "to have power over" something, and in this case, indicates a consumer's ability to exercise some measure of power over, and influence the use of, their data held by another party.[92] While this control provides a person the power to *potentially* effectuate a given result, it does not ensure it. This is different from the RTBF, which focuses on the concept of automatic deletion over time to replicate long-term human memory loss.[93] If a person controls their data under a RTD regime, they could submit a deletion request; however, they may choose not to for a variety of reasons, such as indifference to the possession of the data by another party, an ongoing economic relation, or even the efficiency of resuming an ongoing relationship in the future.

88. § 6-1-1303(17)(a)-(b).
89. Conley, *supra* note 65, at 54.
90. *Id.*
91. *Id.* at 57.
92. *Control*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/control [https://perma.cc/QY7P-MCSW] (last visited Feb. 1, 2022); *see also Control*, BLACK'S L. DICTIONARY (11th ed. 2019) ("To exercise power or influence over.").
93. Jefferies, *supra* note 10.

Second, the RTBF targets broad narratives a party seeks to have removed from *society's* digital memory.[94] In contrast, the RTD is content-neutral in its potential scope, and a party may seek to delete aggregate data that may collectively establish a narrative or target smaller or, on the other hand, specific types of information they simply no longer wish a data holder to have. This can happen for any variety of reasons, such as minimizing how many vendors have their email address or cellphone number. If the RTBF reflects societal values between an individual and their community at large, the RTD reflects a societal goal of allowing individual market participants to exit at any time—but to exit cleanly requires deletion of one's personal data given to a service provider.

Third, as the RTBF focuses on the erasure of narratives, the right itself is concerned with the relationship between an individual and society at large—even when a dispute is between two private parties (in this case, an individual and a data holder). The data holder is the target of the erasure request, but the relationship impacted is between the individual and the community's view of them. Here, the RTD starkly diverges, as the relationship impacted is nearly entirely between two private parties in a transactional sense with no wider societal implication.

Lastly, the RTBF and the RTD are different in their technical implementation. The RTBF can be achieved in a number of ways, but the most commonly-advocated methods are either requiring automatic erasure—creating a digital clock to replicate the non-digital nature of memory to all data—or other measures, such as de-listing, as held in *Google Spain*.[95] In the first case, such a technical rule is a single rule for all personal data. In the second case, a de-listing request interrupts the ability for a local community to find a past, and *now forgotten* narrative of one of its own, even if the narrative itself is retained somewhere online. In contrast, a deletion request under the RTD targets the data itself at its final stored location and has a greater sense of finality than de-listing. Additionally, reflecting the policy goal of granting a consumer control, a deletion request under the RTD is ad hoc, may be made at any time, and may only target a fraction of the data held by the data holder.[96] At the aggregate level, such an ad hoc nature is random in comparison to a RTBF automatic timer.

---

94. *E.g.,* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶¶ 14-15 (May 13, 2014) (where Mr. Gonzales sought to have the narrative of his past financial foreclosures forgotten as part of his present self's re-invention); *see generally* Kodde, *supra* note 14, at (where the information targeted for deletion was generally descriptive information such as a name, background information, gender, past work experience, etc., but the narrative targeted was one of a denied job application that the petitioner sought to prevent from impacting future job search prospects); *see also* Martin v. Hearst Corp., 777 F.3d 546, 548-49 (2d Cir. 2015) (where in the United States, the plaintiff, while denied, sought to fully close the chapter of a past arrest without conviction and remove the narrative from her present-day life and community). For further discussion on narratives, *see* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, PRIVACY ON THE INTERNET 15-102 (2007).

95. *Supra* text accompanying notes 21-25.

96. *Supra* text accompanying note 66, and II.B.2.

III. ANALYSIS

Having distinguished the RTD from the RTBF, the next question is how effective the RTD is at achieving a privacy rights regime's intended goals. As the first RTD was enacted only four years ago, there is negligible quantifiable data or cases to objectively measure its impact.[97] Instead, while an objective or quantifiable study might not yet be feasible, a qualitative analysis of the RTD's limitations and structure—from its procedure and exceptions to other drafting provisions—is possible. This qualitative analysis allows for reforms now, while the right is still in its infancy and yet to be widely adopted across the United States.

A. The Harm of No Standard Technical or Legal Definition of "Delete"

When a consumer exercises their RTD and submits a request to a company, they probably think that their data will be deleted permanently and irretrievably, and that this standard of deletion is uniform across state privacy laws. This consumer presumption is likely incorrect, and typically, "a user's commonsense understanding of the command to 'delete' differ[s] from companies' practices."[98] Beyond consumers, "employees who would be trusted to carry out these technical [deletion & data disposal] tasks often lack basic training on how to do them."[99] Legislators seeking to improve the efficiency of the RTD and strengthen its impact should better regulate and define deletion standards for covered entities. There are three main obstacles to resolving ambiguities on what deletion standard is owed to a consumer: (1) the lack of uniform data deletion and disposal standards; (2) the RTD's interaction with a legal regime that, by design and incentive, prefers data retention; and (3) the variance of technical deletion methods and the financial burden of different deletion methods.

97. Early signs show a low usage of the RTD under the CCPA, with a relatively small number of annual requests submitted so far against the majority of Fortune 500 companies. *See* David A. Zetoony, *How Many Deletion Requests Do Retailers Receive on Average Each Year*?, GREENBERG TRAURIG (Sept. 13, 2021), https://www.gtlaw-dataprivacydish.com/2021/09/how-many-deletion-requests-do-retailers-receive-on-average-each-year/ [https://perma.cc/PX6N-ARCQ]. The vast majority of requests targeted at most only three companies. *Id.*

98. MICHELLE DE MOOY ET AL., CTR. FOR DEMOCRACY & TECH., THE LEGAL, POLICY AND TECHNICAL LANDSCAPE AROUND DATA DELETION 3 (2017), https://cdt.org/wp-content/uploads/2017/02/2017-02-23-Data-Deletion-FNL2.pdf [https://perma.cc/52JZ-R6DY].

99. *Id.* at 6; *see also* Thomas Brewster, *500 Million Google Phones Fail to Wipe Data on Reset, Claim Cambridge Researchers*, FORBES (May 22, 2015, 10:31 AM), https://www.forbes.com/sites/thomasbrewster/2015/05/22/google-android-phones-fail-to-delete-data-on-reset/ [https://perma.cc/6GXT-D7QT].

1. There is No Standard Legal Rule Governing Deletion and Data Disposal

The majority of states have enacted some form of data disposal laws (though some have not been passed or amended recently).[100] Already, there is inconsistency across bills as to whether the controlling data disposal laws apply to both businesses and government,[101] businesses but not to government,[102] or only to government and not to business.[103] Since the RTD is now law in at least three states,[104] the standard for a deletion request by a consumer or covered entity is the corresponding state records and disposal law.

The California data disposal law, as amended in 2009, states that:

> A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[105]

While the disposal provision provides some specificity on the technical standard to be met (namely, rendering the data unreadable or undecipherable), it is also tied to a definition of "personal information," which may exclude data that a consumer assumes would be deleted and may also be inconsistent with the definition of "personal information" under the CCPA.[106] Consequently, the burden shifts to the consumer to research multiple provisions of two state laws to determine if the data they seek to have deleted is covered, the tedious nature of which is inconsistent with the RTD's emphasis on control and direction over one's own data by a consumer.[107]

In contrast to California, the Virginia data disposal law is far less controlling on what standard is required in response to a deletion request. First, the state's data disposal laws only require the Virginia Information

---

100. *Data Security Laws | Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (last updated May 29, 2019) https://www.ncsl.org/technology-and-communication/data-security-laws-private-sector [https://perma.cc/XG5K-HW8Y] ("more than half the states also have enacted data disposal laws that require entities to destroy or dispose of personal information so that it is unreadable or indecipherable). For a list of state governmental disposal statutes *see Data Security Laws | Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (last updated May 29, 2019) https://www.ncsl.org/technology-and-communication/data-security-laws-state-government [https://perma.cc/8H8D-P9X8].

101. *E.g.,* ALA. CODE § 8-38-10 (2018); MICH. COMP. LAWS ANN. § 445.72(a) (West 2007).

102. *E.g.,* IND. CODE ANN. §§ 24-4-14-8, 24-4.9-3-3.5(d) (West 2021); NEB. REV. STAT. § 87-808(1) (West 2006).

103. *E.g.,* VA. CODE ANN. § 2.2-2009 (West 2020).

104. *Supra* note 1, and 4.

105. CAL. CIV. CODE § 1798.81 (West 2020).

106. CIV. § 1798.81.5.

107. *See supra*, II.C. Contrasting the Right to be Forgotten and the Right to Delete.

Technologies Agency Chief Information Officer ("CIO") to provide technical guidance regarding "the development of policies, standards, and guidelines," which can be changed by a subsequent CIO.[108] Second, the law and any CIO guidance applies only to the "Commonwealth's executive, legislative, and judicial branches and independent agencies,"[109] a narrower body of entities than those covered by the VCDPA's RTD. Thus, Virginia's data disposal law is both not controlling for RTD requests and is potentially subject to repeated changes from one CIO to another.

Colorado's code governing disposal of personal identifiable information ("PII") was amended in 2018 to include electronic documents and requires covered entities to develop policies for the destruction and disposal of records containing PII.[110] The Colorado regime, like the California disposal regime, applies broadly to covered entities but provides little specificity as to what constitutes proper disposal for electronic records containing PII.[111] Also like the California disposal regime, the Colorado governing rule has its own definition of PII and is at risk of subsequent inconsistencies between personal data covered under the CPA's RTD and the state's disposal rules.[112]

At the federal level, many authorities dealing with privacy, cybersecurity, data protection, and other substantive areas provide instructions, optional rules, and guidance concerning data disposal. For example, the Department of Health and Human Services ("HHS") has issued guidance on the disposal of protected health information pursuant to the

108. VA. CODE ANN. § 2.2-2009(F) (West 2020) ("The CIO shall provide technical guidance to the Department of General Services in the development of policies, standards, and guidelines for the recycling and disposal of computers and other technology assets. Such policies, standards, and guidelines shall include the expunging, in a manner as determined by the CIO, of all confidential data and personal identifying information of citizens of the Commonwealth prior to such sale, disposal, or other transfer of computers or other technology assets.").

109. § 2.2-2009(I)(1).

110. COLO. REV. STAT. ANN. § 6-1-713(1) (West 2018) ("Each covered entity in the state that maintains paper or electronic documents during the course of business that contain personal identifying information shall develop a written policy for the destruction or proper disposal of those paper and electronic documents containing personal identifying information. Unless otherwise required by state or federal law or regulation, the written policy must require that, when such paper or electronic documents are no longer needed, the covered entity shall destroy or arrange for the destruction of such paper and electronic documents within its custody or control that contain personal identifying information by shredding, erasing, or otherwise modifying the personal identifying information in the paper or electronic documents to make the personal identifying information unreadable or indecipherable through any means.").

111. *See* § 6-1-713.

112. *E.g.,* § 6-1-713(2)(b) (defining PII as a "social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in section 6-1-716(1)(a); an employer, student, or military identification number; or a financial transaction device as defined in section 18-5-701(3)").

HIPAA Breach Notification Rule.[113] The guidance deals not with data deletion itself, but rather provides a standard for rendering protected health information "unreadable, or indecipherable to unauthorized persons."[114] Electronic protected health information ("PHI") must be encrypted consistent with a standard approved by the National Institute of Standards and Technology ("NIST"); PHI stored on physical media (paper, film, or electronic media) must be destroyed by one method from an enumerated list.[115] In contrast to HHS's approach, the Federal Trade Commission ("FTC") has established a mandate for data disposal under the Fair and Accurate Credit Transactions Act ("FACTA").[116] However, while the FACTA disposal requirement is a mandate, it provides far less specificity on the standards for data disposal or deletion, only requiring covered persons or entities to "properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[117]

2. The Right to Delete is Opposed to the Core Design of Legal and Technical Data Disposal Rules

Legislators and policy makers should acknowledge that the RTD is inapposite to the current legal environment and technical design of systems governing data collection, storage, and processing. First, there is currently an inherent bias in favor of big-data collection and storage, as "[i]ncreasingly, data assets are the engine driving the total value and growth of modern

113. HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414 (2009); *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/URL7-88TC] (last visited Nov. 14, 2022) ("Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.").

114. 45 C.F.R. § 164.402 (2009).

115. *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html [https://perma.cc/SPH5-3GQ9] (last visited Mar. 5, 2022); *see also What Do the HIPPA Privacy and Security Rules Require of Covered Entities When They Dispose of Protected Health Information?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Feb. 18, 2009), https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html [https://perma.cc/X8AS-ZLJR] (requiring that "workforce members receive training on . . . disposal policies and procedures . . ." and providing guidance on appropriate disposal standards, depsite the absence of a mandate for covered entities to dispose of PHI).

116. FTC Disposal of Consumer Report Information and Records, 16 C.F.R. pt. 682 (2007); *see also* Press Release, Fed. Trade Comm'n, FACTA Disposal Rule Goes into Effect June 1 (June 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1 [https://perma.cc/YF5Z-W4ZW].

117. 16 C.F.R § 682.3(a) (defining "Standard").

organizations."[118] Beyond the value of individual data profiles of consumers, companies see a myriad of big-data analytic opportunities to use aggregate consumer profiles for improved product and service performance, cost improvement, and new value and derived insights.[119] Consequently, entities covered by privacy statutes are typically incentivized by the market to maximize their digital data collection practices.

Second, numerous sectoral laws require companies to preserve records, from accounting and financial documents to other transactions for law enforcement and civil government administration.[120] Additionally, companies themselves have favored storage in preparation for potential litigation, as the rise in e-discovery costs demonstrates.[121] Unfortunately, historical focus has been on effective record management in preparation for future litigation, [122] rather than on what is essential to save and what is not. However, contrary to current data retention practices, the over-collection of data can "leave[] companies open to serious consequences."[123] One study found that only "one percent of data needs to be retained for litigation purposes," and that up to "70 percent of a company's data assets serve mostly to create liability."[124]

Third, online data use and storage disfavors deletion given the technical challenges of data erasure and the rise of built-in data retrieval technologies.[125] This issue extends from data collection and storage design to data sets themselves in machine learning and AI, where individual data

118. DELOITTE, DATA VALUATION: UNDERSTANDING THE VALUE OF YOUR DATA ASSETS 2 (2020), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Finance/Valuation-Data-Digital.pdf [https://perma.cc/Q5XE-2526].

119. *See* THOMAS H. DAVENPORT & JILL DYCHÉ, INT'L INST. FOR ANALYTICS, BIG DATA IN BIG COMPANIES 3 (2013), https://docs.media.bitpipe.com/io_10x/io_102267/item_725049/Big-Data-in-Big-Companies.pdf [https://perma.cc/B82V-VMFZ%5d].

120. *E.g.,* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 802, 116 Stat. 745, 800-01 (2002) (governing the record-keeping obligations of accounting and financial auditors).

121. John H. Beisner, *Discovering a Better Way: The Need for Effective Civil Litigation Reform*, 60 DUKE L.J. 547, 585 (2010) ("[T]he ubiquity of modern computer systems—and the ever-growing caches of information they contain—has led to a tremendous surge in the costs of electronic discovery.").

122. *See, e.g.*, Steven C. Bennett, *Records Management: The Next Frontier in E-Discovery*, 41 TEX. TECH L. REV. 519, 522 (2009) (analyzing how "[e]ffective [records management] can dramatically improve the e-discovery process," and how "[w]ell organized information can be more easily and cheaply gathered, searched, reviewed, and produced" and not how companies can efficiently delete non-essential data and preserve the truly relevant and required data).

123. DE MOOY ET AL., *supra* note 98, at 7.

124. *Id.*

125. Technology service providers often provide guidance or applications to recover files after a consumer has theoretically deleted them. *E.g., Recover Lost Files on Windows 10*, MICROSOFT, https://support.microsoft.com/en-us/windows/recover-lost-files-on-windows-10-61f5b28a-f5b8-3cc2-0f8e-a63cb4e1d4c4 [https://perma.cc/S8R4-ZT2V] (last visited Mar. 5, 2022); *Move Files to Trash and Restore Files from Trash*, FILES BY GOOGLE, https://support.google.com/files/answer/10607740 [https://perma.cc/D86W-M3HJ] (last visited Mar. 5, 2022).

deletion requests are particularly opposed.[126] This is related to the next critical issue the RTD faces, which is the difficulty in deletion itself and its various definitions and methods.

3. Technical Definitions and Methods of Deletion Vary

There are material differences between various technical and legal standards of deletion, particularly given inconsistent standards for responding to a deletion request. Traditional deletion methods for data held on individual devices include (1) the command delete, which "removes pointers to information on your computer, but . . . does not remove the information"; (2) overwriting, which "puts random data in place of your information . . . [that] cannot be retrieved because it has been obliterated"; and (3) physical destruction.[127] Further, some deletion standards and recovery tools focus on individual hardware data[128] and thus are likely inapplicable for the majority of covered entities who would receive a request. As data has migrated to cloud computing services, over-writing and other cryptographic erasure techniques[129] have become more prominent, with physical destruction only available for companies seeking to destroy an entire data set or asset. Google's Cloud system uses multiple deletion methods depending on the product or data marked for deletion.[130] Cloud-stored data is deleted through both cryptographic erasures and overwriting, where copies of the data are

126. *See* Antonio A. Ginart et al., *Making AI Forget You: Data Deletion in Machine Learning*, *in* ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS 32: PROCEEDINGS OF THE 2019 CONFERENCE 3502, 3504-508 (Hanna M. Wallach et al. eds., 2019) (discussing the value of deletion efficiency within general learning algorithms and proposing two deletion efficient solutions).

127. LINDA PESANTE ET AL., U.S. COMP. EMERGENCY READINESS TEAM, DISPOSING OF DEVICES SAFELY 2 (2012), https://www.cisa.gov/uscert/sites/default/files/publications/DisposeDevicesSafely.pdf [https://perma.cc/7UEN-7G79].

128. For instance, there are deletion methods and recovery tools more focused on an individual device, such as a laptop or phone, that would likely be irrelevant to a data deletion request to a company which might store data via one or even many cloud-storage companies. One example is DiskDigger, a free tool that helps recover Windows files from a specific laptop and is often used in gathering forensic evidence by law enforcement. CHUCK EASTTOM, COMPUTER SECURITY FUNDAMENTALS 399 (Mark Taub et al. eds., 4th ed. 2020).

129. Cryptographic deletion is a two-stage process. First, data is encrypted in a procedure to "scramble information so that only someone knowing the appropriate secret [an encryption key] can obtain the original information . . . ." CHARLIE KAUFMAN ET AL., NETWORK SECURITY: PRIVATE COMMUNICATION IN A PUBLIC WORLD (Faye Gemmellaro et al. eds, 2d ed. 2002). Second, during the erasure process, rather than overwriting data, the encryption key is erased using "similar overwriting methods." *Id.* The process prevents description of the data and requires overwriting of only data keys, a smaller volume to overwrite, than the full data itself. *See* Sarah M. Diesburg & An-I Andy Wang*, A Survey of Confidential Data Storage and Deletion Methods*, 43 ACM COMPUTING SURVS., no. 1, 2010, at 1, 4, 28.

130. *Data Deletion on Google Cloud*, GOOGLE CLOUD, https://cloud.google.com/docs/security/deletion [https://perma.cc/4F9M-A3BQ] (last visited Mar. 6, 2022).

marked as "storage and overwritten over time."[131] Amazon employs similar techniques but denotes data blocks (digital storage room) to be wiped only "immediately before reuse" which can give the appearance that something has been deleted when the act of deletion has yet to occur.[132]

4. Recommendations

In reviewing the legal and technical environment surrounding deletion, it is clear that (1) there is likely a disconnect between consumer understandings of deletion and legal deletion under state law and (2) consumers and covered entities have a myriad of authorities they must consult for guidance on both legal coverage and technical standards to execute data deletion requests under the RTD. Bridging the gap between consumers' expectations and reality and simplifying compliance for covered entities is essential for the RTD to be effective.

A starting point on the legal side of deletion is to adopt a more standardized definition. While this is a common refrain to privacy law reform discussions, it is particularly salient for deletion requirements considering the technical nature of compliance. First, legislators should harmonize the different approaches to deletion. This means that rather than states adopting different examples or standards to define "reasonable steps" for data deletion or record disposal, all states should consider adopting a single approach.[133] Second, legislators should ensure that the scope of their state privacy bills—from covered entities to the definitions of PII—match any equivalent controlling state data and records disposal laws. This would correct ambiguous gaps, such as in Virginia, where the disposal guidance is controlling only to governmental agencies and not to all entities covered under the VCDPA.[134] There is an inherent difficulty in aligning state rules and compliance, as individual states fiercely protect their own approach.[135] However, the RTD (perhaps more than the other rights under recent privacy bills) is normally focused on re-balancing the control between consumers and data-holders. The more difficult compliance is for companies that operate nationally, the more such a re-balance of control is undermined.

While improved consistency in legal standards is required, too much specificity is neither desirable nor reflective of the constant evolution of data

131. *Id.*

132. AMAZON WEB SERVS., OVERVIEW OF AWS SECURITY – COMPUTE SERVICES 7 (2016) [hereinafter OVERVIEW OF AWS SECURITY], https://d0.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf [https://perma.cc/NX2Z-7LNP].

133. *E.g.,* DEL. CODE ANN. tit. 19, § 736(b) (West 2015).

134. *See supra* notes 107-08 and accompanying text.

135. *E.g.*, Letter from Rob Bonta, Attorney General, State of California, and Nine Attorneys Generals to Congressional Leaders (July 19, 2022), https://cppa.ca.gov/meetings/materials/20220728_item2_letter_attorney_general.pdf [https://perma.cc/EXL8-49HC] (arguing against the proposed federal preemption of the 2022 American Data Privacy and Protection Act bill in contemplation by Congress and encouraging Congress to "adopt a federal baseline, and continue to allow states to make decisions about additional protections for consumers residing in their jurisdictions").

management and technology. A compromise for state legislators is to defer technical standards to an alternative body. NIST would be an ideal candidate for such an approach. NIST has substantial technical competency that would be difficult for state legislators to match in determining standards. More importantly, NIST has taken an enlarged role in recent years, having published guidance in the cyber, privacy[136] and computing environment. And many of the largest service providers already comply with NIST standards.[137] Such an approach would harmonize standards and technical competence and reduce compliance complexity for data holders operating under various privacy regimes and data deletion requests. An additional benefit of NIST standards is the flexibility they would provide to the range of covered entities. Deletion is not a binary process; it entails a range of methodologies that contain many tradeoffs.[138] Covered entities range in type and scale, and a one-size-fits-all approach to deletion may increase costs and difficulties for some organizations beyond the benefit provided to consumers. NIST is well-suited to mitigate this risk, as many of their standards reflect the disparate needs of organizations reliant on their guidance. For instance, both the NIST Cybersecurity and Privacy Frameworks create organizational profiles and menus of technical options and approaches reflective of the circumstances of individual organizations.[139] While states themselves might be reluctant to create a rights-based privacy regime dependent on a federal body they have no influence or control over, this approach might provide the most balanced improvement to RTD. Such an idea might be gaining traction, with one proposed state privacy bill already attempting to incorporate NIST standards into its regime.[140]

B. The Risk of De-identification Exemptions to The Right to Delete

Another area for legislators to address to improve the RTD is the risk of anonymization exemptions to deletion requests in the face of the progress made in re-identification science and methodologies. A common exemption to the scope of personal data—and any related rights that might turn on a

136. *See generally* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NIST 800-88, GUIDELINES FOR MEDIA SANITIZATION (2014), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf [https://perma.cc/RCG5-BQBR].

137. OVERVIEW OF AWS SECURITY, *supra* note 131, at 7.

138. Diesburg & Wang, *supra* note 128, at 30.

139. *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0, 8 (2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf [https://perma.cc/PC4Z-CH4E]; NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.1 v-vi, 11 (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/JA76-KWPV].

140. *E.g.,* H.B. No. 376, 134th Gen. Assemb., Reg. Sess. § 1355.11(I)(1)(a)(i) (Ohio 2022) (proposing under the Ohio Personal Privacy Act an affirmative defense for a covered entity that "reasonably conforms to the [NIST] privacy framework").

definition of personal data or PII—is de-identified (also anonymized and/or pseudonymized) data.[141] Under the CCPA, a deletion request does not extend to personal data that is "deidentified or [converted to] aggregate consumer information."[142] Both the CPA and VCDPA contain the same de-identification exemption.[143] Historically, de-identification "has been the main paradigm used in research and elsewhere to share data while preserving people's privacy."[144] Unfortunately, regulators and "legal scholars share [a] faith in anonymization" that does not reflect recent trends and progress in re-identification science.[145]

De-identification as a free pass to deletion for business and data-processors, combined with "the power of reidentification[,] will create and amplify privacy harms" and potentially undermine the purpose of empowering consumers with more control over their personal data.[146] Even in the early 2000s, companies were relying on de-identification to expose private data under the gaze of external research, such as the AOL research data set that allowed for the re-identification of its data set objects who were users in the study.[147] Privacy regimes refer to de-identified data not in absolute terms, but as data that cannot be reasonably re-identified. The reality is that it is relatively easy to re-identify data. One recent study compared different methodologies of re-identification to determine the likely success of re-identification; crucially, the study found that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes."[148]

---

141. Provisions for de-identification exemptions and methods are common in federal laws and regulations. *See, e.g.*, OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 5-6 (2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf [https://perma.cc/C6NK-R6WS]; *see also* PRIV. TECH. ASSISTANCE CTR., U.S. DEP'T OF EDUC., DATA DE-IDENTIFICATION: AN OVERVIEW OF BASIC TERMS 3 (2012), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms.pdf [https://perma.cc/S749-P6VD].

142. CAL. CIV. CODE § 1798.140(v)(3) (West 2020).

143. *See* VA. CODE ANN. § 59.1-571 (West 2021); COLO. REV. STAT. ANN. § 6-1-1303(17)(b) (West 2021).

144. Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 NATURE COMM., no. 3069, 2019, at 1, 2.

145. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1710-11 (2010).

146. *Id.* at 1705.

147. Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), https://www.nytimes.com/2006/08/09/technology/09aol.html [https://perma.cc/2TKW-N7NF] (reporting that amongst other re-identification efforts, a single user was identified as an example of the privacy harm AOL's release of supposedly protected anonymized data had unleased).

148. Rocher et al., *supra* note 143, at 1; *see also Too Unique to Hide*, NATURE COMM., https://cpg.doc.ic.ac.uk/individual-risk/ [https://perma.cc/P5DR-36CN] (last visited Nov. 15, 2022) (featuring an online tool developed by the authors of the source in note 143 that allows U.S. and U.K. residents to test whether they can already be re-identified).

Without entirely blocking the value of anonymized data for researchers,[149] legislators must acknowledge that the protection level of de-identification is weaker than assumed and take a second look at how broadly such an exemption should apply to privacy rights, such as the RTD, in the context of truly empowering consumers to control their personal data.

C. An Alternative Path: Market Incentives To Collect & Retain Less Consumer Data

While the previous two sections focused on areas of improvement for the RTD, policymakers should also keep in mind the limitations to what the RTD can address. This Note has argued that the RTD can and should be strengthened, but ultimately it is only one right in a legal regime that focuses on providing consumers more measurable control over their personal data, which is distinct from wide-spread data protection.

Regardless of the policy goals of the RTD, "rights are often asked to do far more work than they are capable of doing."[150] Legislators and regulators should consider going beyond addressing gaps in the current design of the RTD and consider engaging with businesses directly to encourage practices that reduce the scope of data collected ahead of subsequent consumer deletion requests.

Going beyond strengthening privacy rights, there are three arguments that legislators and regulators can deploy in such deliberations with business or regulatory bodies that collect and store vast amounts of personal data. First, companies must embrace the paradigm shift that they *will* be breached and risk exposing their data assets and consumer personal data.[151] Businesses and governmental data-holding bodies cannot ignore their centrality in societal privacy protections and assume that they will not be drawn into the fray.[152] Second, *when* a cyber breach does occur, there is now a large body of authorities that govern the response, particularly the evidence and forensic gathering steps that breached organizations must adhere to. These range from

149. *See* CERT Podcast Series: Security for Business Leaders, *The Value of De-Identified Personal Data*, SOFTWARE ENG'G INST., at 07:50 (May 15, 2007), https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34562 [https://perma.cc/DMC6-9K67] (transcript available for PDF download on linked webpage).

150. Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023) (manuscript at 2) (on file at The George Washington University Law School Scholarly Commons, Paper Series 2022-30).

151. Tyler Anders et al., *Not "If" but "When"—The Ever Increasing Threat of a Data Breach in 2021*, JD SUPRA (July 15, 2021), https://www.jdsupra.com/legalnews/not-if-but-when-the-ever-increasing-8569092/ [https://perma.cc/N7T5-J2BK] ("If the statistics are correct, the question for most companies is not if they will be a victim of cybercrime, but when.").

152. *See* CYBERSECURITY UNIT, U.S. DEP'T OF JUST., BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 1 (2018), https://www.justice.gov/criminal-ccips/file/1096971/download [https://perma.cc/F3TR-YUCR] (discussing the importance of "[h]aving well-established plans and procedures . . . to weather a cyber incident," with less of an emphasis on avoiding possible cyber breaches).

U.S. Secret Service guidance[153] to international law under the Budapest Convention (to which the United States is a party).[154] As previously discussed, when a breach occurs, there is often extensive e-discovery and litigation costs,[155] amplified by the volume of data needlessly exposed because of over-collection and retention practices by firms, which the RTD cannot solve by itself.

Third, to manage this increased liability, there are non-regulatory solutions that firms can employ, whether they decide to collect and retain less data to address privacy harms[156] or are self-incentivized to reduce extremely likely future litigation costs. Organizing vast data sets and deleting irrelevant or low-value data without decreasing the value of a businesses' data assets is possible and desirable.[157] Organizations should look internally to develop or employ newly available tools to reverse track from the existing absolutism that more data is better.

IV. CONCLUSION

Understanding the backgrounds of the RTBF and RTD is critical to distinguishing the two rights and analyzing problems with the RTD. Some of the debate and analysis of the RTBF can be drawn on when analyzing the RTD, but it is ultimately not controlling. The RTD has the potential to help shift the balance of control over one's personal data, but in its current form, will have only a limited effect. A more effective RTD that applies uniformly

---

153. U.S. SECRET SERV. CYBERCRIME INVESTIGATIONS, PREPARING FOR A CYBER INCIDENT: AN INTRODUCTORY GUIDE (2020), https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20An%20Introductory%20Guide%20v%201.1.pdf [https://perma.cc/BH98-3QFB].

154. The Budapest Convention on Cybercrime, passed by the Council of Europe, discusses electronic evidence gathering for possible criminal offenses. *The Budapest Convention (ETS No. 185) and Its Protocols*, COUNCIL OF EUR., https://www.coe.int/en/web/cybercrime/the-budapest-convention [https://perma.cc/WAT9-UH44] (last visited Sept. 21, 2022).

155. *See supra* notes 110-11 and accompanying text.

156. *See Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises*, IDENTITY THEFT RES. CTR. (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ [https://perma.cc/9UHC-KTPF%5d] (reporting that the number of "data compromises" in 2021 was 23 percent over the previous all-time high).

157. For example, Dare2Del is a product that helps "to regulate [] digital knowledge by hiding and deleting irrelevant digital objects such as files or sensor data." *DFG-Project Dare2Del*, GERMAN RSCH. FOUND., https://dare2del.de/ [https://perma.cc/WE87-A7WX] (last updated Nov. 16, 2020). In an associated publication, the research team outlines the methodology of the tool which focused on relational irrelevance — the process of determining when data or files are "irrelevant" in their relation to current high value data, and then proposes to a system administrator to de-list or delete such data based on first order logic. Michael Siebers & Ute Schmid, *Please Delete That! Why Should I?*, 33 KI - KÜNSTLICHE INTELLIGENZ, 2019, at 35, 35-36. This tool is currently equipped for small scale data operations and is illustrative of the potential for more large-scale operation market solutions that can redress the liability balance for organizations holding vast amounts of consumer data..

and to a large scope of personal data will grant consumers a more pronounced measure of control. This Note has argued that if legislators only address deletion standards and avoid the broad exemption of deidentified data alone, then the RTD's potential will be more substantially realized than in its current form.