William & Mary Law Review

Volume 62 (2020-2021)
Issue 2

Article 6

11-2020

Data of the Dead: A Proposal for Protecting Posthumous Data Privacy

Kate C. Ashley

NOTES

DATA OF THE DEAD: A PROPOSAL FOR PROTECTING POSTHUMOUS DATA PRIVACY

TABLE OF CONTENTS

INTRODUCTION

On January 1, 2020, a sweeping set of new consumer protections took effect in California.[1] The California Consumer Privacy Act (CCPA) breaks new ground in empowering consumers with the tools necessary to protect their data privacy.[2] Modeled partially after the European Union's General Data Protection Regulation (GDPR),[3] CCPA has been criticized for not going far enough,[4] while affected industries (including search engine and social media companies) have generally regarded the bill's enactment as the end times.[5] CCPA enjoys strong support among Californians, with 88 percent in favor of the legislation.[6] However, one group of affected consumers has been altogether reticent on the matter—the dead.

Though the deceased are unable to register opinions of any variety following their demise, it is foundational to many aspects of the law that the dead's wishes and rights be observed. Consider, for example, the area of trusts and estates, in which individuals may express their wishes for the settlement of their property in the event of their death, or the numerous dignitary statutes that criminalize desecration of human remains.[7] This Note argues that data privacy rights should be included in the privacy, property, and dignitary interests that the law extends posthumously.

---

1. *See* Jeff John Roberts, *Here Comes America's First Privacy Law: What the CCPA Means for Business and Consumers*, FORTUNE (Sept. 13, 2019, 6:30 AM), https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law/ [https://perma.cc/H8AS-GU8X].

2. *See id.*

3. *See* Tony Howlett, *How GDPR, CCPA Impact Healthcare Compliance*, COMPLIANCE WK. (Aug. 12, 2019, 3:46 PM), https://www.complianceweek.com/data-privacy/how-gdpr-ccpa-impact-healthcare-compliance/27558.article [https://perma.cc/Z2TX-8UUK].

4. *See, e.g.*, Jazmine Ulloa, *California Has Become a Battleground for the Protection of Consumer Privacy Rules*, L.A. TIMES (Mar. 11, 2019, 12:05 AM), https://www.latimes.com/politics/la-pol-ca-california-privacy-law-battles-20190311-story.html [https://perma.cc/G7KM-ZQLR].

5. *See id.*

6. Odia Kagan, *Poll Shows Strong Public Support in California for CCPA, Even Stronger Privacy Laws*, JD SUPRA (Oct. 22, 2019), https://www.jdsupra.com/legalnews/poll-shows-strong-public-support-in-24081/ [https://perma.cc/F79Q-VLSG].

7. *See generally* Kirsten Rabe Smolensky, *Rights of the Dead*, 37 HOFSTRA L. REV. 763, 763-66 (2009) (discussing how the legal rules affecting the dead often stem from cultural norms).

First, a brief overview of what is meant by data privacy rights will help clarify the following analysis. Data privacy laws (both domestically and abroad) "govern[] the collection, use, processing, preservation, and divulgence of personal information."[8] In statutes, personal information often means "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information."[9] The private sector has defined personal information as including

> (1) name, address, email address, phone number, (2) race, nationality, ethnicity, origin, color, religious or political beliefs or associations, (3) age, sex, sexual orientation, marital status, family status, (4) identifying number, code, symbol, (5) finger prints, blood type, inherited characteristics, (6) health care history including information on physical/mental disability, (7) educational, financial, criminal, employment history, (8) others' opinion about the individual, and (9) personal views except those about other individuals.[10]

However, data privacy is not limited to just the information covered in statutes like the Driver's Privacy Protection Act[11] and the Video Privacy Protection Act.[12] As enumerated in CCPA, personal information includes the myriad data that businesses collect on individuals: "where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks."[13] This kind of deeply personal information fuels artificial intelligence recommendations for prospective dates and new varieties of dog

---

8. Samantha Cutler, *The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law when Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1514 (2018).

9. 18 U.S.C. § 2725(3).

10. *Personal Information*, BUSINESSDICTIONARY, http://www.businessdictionary.com/definition/personal-information.html [https://perma.cc/ZS6U-CRKT].

11. 18 U.S.C. § 2721.

12. *Id.* § 2701.

13. California Consumer Privacy Act of 2018, ch. 55, § 2(e), 2018 Cal. Stat. 1807, 1809.

food, reminders of upcoming birthdays and anniversaries, and predictions on optimal fertility windows.[14] The amount and scope of information businesses collect about individuals rivals (and likely exceeds) what even our closest friends, family, and romantic partners know about us.[15]

Identifying the right to privacy as an "'inalienable' right[ ] of all people,"[16] California leads the way in protecting the kinds of information that many among us would consider deeply personal. This is the kind of information that some would prefer was never revealed—even after death.[17] Generally, American culture has understood this desire and has created legal protections to honor this posthumous wish when it has been expressed. For example, many public figures place their private papers under seal for a certain number of years following their death[18] or require the destruction of their personal papers.[19]

Before American society transformed into an increasingly digital culture, honoring a decedent's intent with respect to personal papers and information was fairly straightforward and typically entailed taking possession of the physical papers, mail, and documents found at the decedent's residence and office, following the decedent's wishes.[20] Today, most of one's "papers" live electronically in cloud storage, email accounts, and various social media profiles.[21] The law remains unsettled on how to regard an individual's digital effects, as courts determine whether these digital assets are more like

14. *See* Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BLOGS (Oct. 29, 2018), https://blogs.harvard.edu/jzwrites/2018/10/29/how-to-exercise-the-power-you-didnt-ask-for/ [https://perma.cc/TPA6-7F66].

15. *See* Tim Herrera, *How to See What the Internet Knows About You (and How to Stop It)*, N.Y. TIMES (July 3, 2017), https://www.nytimes.com/2017/07/03/smarter-living/how-to-see-what-the-internet-knows-about-you.html [https://perma.cc/FNU5-NXJX].

16. California Consumer Privacy Act of 2018 § 2(a) (quoting CAL. CONST. art. 1, § 1).

17. *See* Sara S. Hodson, *In Secret Kept, in Silence Sealed: Privacy in the Papers of Authors and Celebrities*, 67 AM. ARCHIVIST 194, 195 (2004).

18. *See id.* at 196.

19. Consider, for example, Franz Kafka, whose will instructed his executor to destroy all his unpublished work (including *The Metamorphosis*). *See* Elif Batuman, *Kafka's Last Trial*, N.Y. TIMES MAG. (Sept. 26, 2010), https://www.nytimes.com/2010/09/26/magazine/26kafka-t.html [https://perma.cc/8R4B-EVV8]. Ultimately (and ironically), the executor ignored Kafka's instructions and published several of his works. *See id.*

20. *See* Ajemian v. Yahoo!, Inc., 84 N.E.3d 766, 773-79 (Mass. 2017).

21. *See* Natalie M. Banta, *Death and Privacy in the Digital Age*, 94 N.C. L. REV. 927, 927 (2016).

property or are something else altogether.[22] However, a vast trove of personal data currently exists beyond the control of any individual: the personal information created about an individual but not created by that individual. This is the very information CCPA was designed to protect,[23] but the law's scope contains a significant gap. While CCPA empowers individuals to control this personal data in their lifetime,[24] CCPA stops short of empowering the personal representatives of decedents to exercise control over personal data according to the decedent's wishes.

This Note will focus on the posthumous disposition of the personal information businesses collect, use, and sell about individuals and argue that data privacy rights should extend posthumously to fulfill the promise of data privacy legislation like CCPA. In Part I, this Note will examine the dead's legal and customary rights, from property rights to cultural observances, to identify the contours of posthumous rights. Part II will shift the analysis to the evolution of data privacy rights in American jurisprudence by tracing the development of CCPA. Part III will weave together the contours of posthumous rights with the development of data privacy rights to argue that data privacy rights must extend posthumously.

I. THE RIGHTS WE OWE THE DEAD

The legal maxim that "the dead have no rights," though pithy, has never been strictly true.[25] The field of trusts and estates exists to ensure a decedent's wishes for the distribution of an estate are honored.[26] The Uniform Anatomical Gift Act requires that the living respect the wishes of the dead vis-à-vis organ donation.[27] Criminal

22. *See* Alberto B. Lopez, *Posthumous Privacy, Decedent Intent, and Post-mortem Access to Digital Assets*, 24 GEO. MASON L. REV. 183, 215-16 (2016).

23. *See* California Consumer Privacy Act of 2018, ch. 55, § 2(e), 2018 Cal. Stat. 1807, 1809.

24. *See id.* § 2(i).

25. *See* Smolensky, *supra* note 7, at 763.

26. *See* LAWRENCE M. FRIEDMAN, DEAD HANDS: A SOCIAL HISTORY OF WILLS, TRUSTS, AND INHERITANCE LAW 3-4 (2009).

27. At this time, forty-six states, the District of Columbia, and the U.S. Virgin Islands have adopted the most recent amendments to the Uniform Anatomical Gift Act. *Anatomical Gift Act*, UNIF. L. COMM'N, https://www.uniformlaws.org/committees/community-home?CommunityKey=015e18ad-4806-4dff-b011-8e1ebc0d1d0f [https://perma.cc/Q2AC-GMTF].

statutes prevent the desecration of dead bodies and burial sites.[28] Many of the legal rules that protect posthumous interests stem primarily from "cultural norms, including dignity and respect for decedents' wishes."[29] A brief examination of three theories of posthumous interests will lay the foundation for a consideration of posthumous data privacy: property interests, dignitary interests, and privacy interests.

A. Posthumous Property Interests

Within reasonable limits, American common law allows individuals to direct the distribution of real property and to condition its uses following an individual's death.[30] So long as testamentary wishes are lawful, a decedent's decisions will generally be honored.[31]

A decedent's beneficiaries may take legal action to enforce the decedent's wishes (even, in some cases, by taking legal action against each other).[32] Suits regarding real property are common enough, while an emerging area of law considers the ownership of digital assets, such as social media profiles and the contents of email accounts.[33] Though analyzing the legal theories of ownership of digital assets remains beyond the scope of this Note, the underlying theory that digital data constitutes property will figure into the discussion to follow.

In addition to the real property a decedent leaves behind, the law also treats the decedent's remains as property.[34] The property

---

28. *See, e.g.*, CAL. HEALTH & SAFETY CODE § 7052(a) (West 2018) ("Every person who willfully mutilates, disinters, removes from the place of interment, or commits an act of sexual penetration on, or has sexual contact with, any remains known to be human, without authority of law, is guilty of a felony."); N.J. STAT. ANN. § 2C:22-1 (West 2002) (specifying a similar prohibition to California's law); N.Y. PUB. HEALTH LAW § 4216 (McKinney 2010) (prohibiting body stealing); S.C. CODE ANN. § 16-17-600 (2010) (similar to California's law).

29. Smolensky, *supra* note 7, at 764.

30. *See* Julia D. Mahoney, *The Illusion of Perpetuity and the Preservation of Privately Owned Lands*, 44 NAT. RES. J. 573, 573-74 (2004). The rule against perpetuities generally limits individuals from commanding the living beyond the grave. *See id.*

31. *See* FRIEDMAN, *supra* note 26, at 4.

32. *See, e.g.*, Marshall v. Marshall, 547 U.S. 293, 300 (2006).

33. *See, e.g.*, Ajemian v. Yahoo!, Inc., 84 N.E.3d 766, 768 (Mass. 2017) (involving a decedent's brother and sister suing Yahoo! for access to their brother's email account).

34. *See, e.g.*, Native American Graves Protection and Repatriation Act, 25 U.S.C. § 3002(a) (establishing that the "ownership" of Native American remains found on federal or tribal land

interests in one's remains are limited to the specification of funerary arrangements (within reason), though as Dahlia Lithwick points out, "[A] will's burial specifications are not probated until long after the funeral."[35] While respect for burial specifications, as a practical matter, veers away from property interests and into the cultural norms and dignitary interests discussed by Professor Smolensky, the treatment of a decedent's likeness is firmly rooted in notions of property.[36]

Though there is no libel of the dead, some jurisdictions empower a decedent's beneficiaries to file libel suits on a theory that a third party has violated the decedent's publicity rights.[37] This theory centers on the notion of "descendible publicity rights" as a form of perpetual right to identity, which becomes a form of property.[38] This theory is grounded more in protecting the living's ability "to create marketable identities and with protecting the financial interests of the decedent's heirs" rather than protecting the decedent's dignitary interests.[39] This claim would be actionable when a libel claim would fail because the injury suffered is concrete: a loss of economic value.[40] Generally, though, the law does not allow for posthumous defamation under the belief that the dead no longer have a reputation and cannot suffer offense.[41]

Though not legally actionable, the cultural taboo against speaking ill of the dead plays a central role in traditions of posthumous dignitary interests. The next Section discusses how concerns for the dignity of the dead have shaped these interests in both cultural norms and state statutes.

---

shall be "in the lineal descendants of the Native American").

35. Dahlia Lithwick, *Habeas Corpses*, SLATE (Mar. 14, 2002, 5:45 PM), https://slate.com/news-and-politics/2002/03/what-are-the-rights-of-dead-people.html [https://perma.cc/9SFH-KYKY]. Lithwick also details the strange case of a French couple who wished to be interred in a refrigerated container in the basement of their chateau. *See id.* A French court ordered their burial or cremation, over the objections of the couple's son. *See id.*

36. *See* Smolensky, *supra* note 7, at 763-64.

37. *See* William H. Binder, *Publicity Rights and Defamation of the Deceased: Resurrection or R.I.P.?*, 12 DEPAUL-LCA J. ART & ENT. L. 297, 299 (2002).

38. *See id.* at 298.

39. Smolensky, *supra* note 7, at 769.

40. *See* Bo Zhao, *Posthumous Defamation and Posthumous Privacy Cases in the Digital Age*, 3 SAVANNAH L. REV. 15, 19 (2016).

41. *See, e.g.*, Rich v. Fox News Networks, LLC, 939 F.3d 112, 125 (2d Cir. 2019).

B. Posthumous Dignitary Interests

American society honors the dead in ways that are deeply embedded within the philosophical discussion over whether the dead have rights.[42] After all, "one measure of any civilized society is how they treat their dead."[43] Whether the treatment of the dead is mandated by statute and enshrined by "rights" or is simply customary, taboos against desecrating human remains and speaking ill of the dead persist.[44] As such, an individual need not specify burial arrangements or express a desire to be free of postmortem humiliation to enjoy these interests posthumously. However, statutes exist to enforce posthumous dignitary interests.[45]

This raises the important question of whom these dignitary interests actually benefit: the dead or their heirs? One may argue, as many have, that just as the dead neither enjoy reputation nor perceive harm postmortem, their dignitary interests extinguish with their life.[46] Others, however, have argued persuasively that the law does not require the perception of harm to constitute a violation of the law.[47] A landowner, to take just one example, suffers trespass whenever an individual enters her land without permission—whether the landowner is aware of the trespass or not.[48] Following this line of argument, the dead suffer a trespass on their dignity whenever it is violated, even if they can no longer be aware of it. For those who do not find this argument persuasive, providing a definitive answer to the question of whom dignitary laws protect is less important for the following analysis than recognizing that American cultural values respecting the dead have shown a willingness to protect their dignity.

Numerous criminal statutes support this interpretation of a trespass to the dead's dignity, including those that prohibit the

42. *See* Smolensky, *supra* note 7, at 763-64.

43. Lithwick, *supra* note 35.

44. Consider, for example, Sophocles's Greek tragedy *Antigone*, which centered on the refusal to treat a fallen foe with customary respect. SOPHOCLES, ANTIGONE 3-9 (David Franklin & John Harrison trans., Cambridge Univ. Press 2003) (c. 441 B.C.E.).

45. *See, e.g.*, *supra* notes 27-28 and accompanying text.

46. *See* JENNIFER E. ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD 156 (2018).

47. *See* Smolensky, *supra* note 7, at 764.

48. *See id.* at 771.

desecration of human remains, sexual intercourse with a dead body, and the theft of a dead body.[49] To ensure proper care of the bodies of the dead, many states regulate the funeral industry, license funeral homes, and regularly inspect crematoriums.[50] The public outcry (and ensuing litigation) over the Tri-State Crematory scandal—in which a crematory operator accepted payment for cremations he never performed, returned fake remains to grieving families, and stashed the remains of over three hundred decedents across his family's property—amply demonstrates the cultural significance of the laws and regulations that protect the sanctity of the bodies of the dead.[51]

In addition to protecting the sanctity of bodies after death, there has long been a culturally recognized norm of restricting the use of images of the dead.[52] The Supreme Court has recognized that "[f]amily members have a personal stake in honoring and mourning their dead and objecting to unwarranted public exploitation that, by intruding upon their own grief, tends to degrade the rites and respect they seek to accord to the deceased person who was once their own."[53] The sad case of Nikki Catsouras demonstrates how these complicated dignitary issues became exacerbated by rapid advances in technology.[54] There, a teenager fatally crashed her car in a gruesome accident.[55] California Highway Patrol (CHP) officers on the scene, following protocol, took pictures of the accident for their report.[56] Those CHP officers then forwarded those images to others and the images went viral.[57] Catsouras's parents, who had

---

49. *See supra* note 28 and accompanying text.

50. *See, e.g.*, CAL. BUS. & PROF. CODE § 7653.2 (West 2016) (granting the state authority to inspect crematories); N.H. CODE ADMIN. R. ANN. FRL. 603.01 (2019) (providing for inspections of funeral homes that perform embalming); N.J. STAT. ANN. § 45:7-33 (West 2019) (requiring embalmers and funeral directors to be licensed).

51. *See* Sara Rimer, *Dazed by Crematory Scandal, Undertakers' Trust Is Shaken*, N.Y. TIMES (Feb. 21, 2002), https://www.nytimes.com/2002/02/21/us/dazed-by-crematory-scandal-undertakers-trust-is-shaken.html [https://perma.cc/M8GB-WLYZ].

52. *See* Nat'l Archives & Recs. Admin. v. Favish, 541 U.S. 157, 167-68, 170 (2004).

53. *Id.* at 168.

54. *See* Jessica Bennett, *For Family of Nikki Catsouras, a Victory in Court*, NEWSWEEK (Feb. 4, 2010, 7:00 PM), https://www.newsweek.com/family-nikki-catsouras-victory-court-75069 [https://perma.cc/V7DB-6SQP].

55. *Id.*

56. *Id.*

57. *Id.*

been prevented from identifying their daughter's remains, were bombarded with these images and filed suit against CHP[58] and the two CHP officers responsible for disseminating the images.[59] Ultimately, a California appeals court, unpersuaded by the officers' claim to have used the images to discourage drunk driving, castigated the officers' "moral[ ] deficien[cy]" in creating a "vulgar spectacle" that inflicted "devastating trauma"[60] and paved the path for an out-of-court settlement.[61] As the litigation following Nikki Catsouras's death revealed, a disregard for the dead's dignity rights can also violate their privacy rights.

C. Posthumous Privacy Rights

The right to privacy is a much more recently developed right, one that has been the subject of some controversy since its articulation in cases like *Griswold v. Connecticut*.[62] As thorny as a right to privacy is for the living, it has an even more complex half-life as a posthumous right. Many scholars argue that the dead have no right to privacy,[63] just as the dead cannot be defamed.[64] However, the law recognizes at least two instances of a posthumous interest in privacy: within the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[65] and the Freedom of Information Act (FOIA).[66]

As the key law regulating health information and privacy, HIPAA primarily focuses on a patient's right to privacy with respect to information regarding their personal health and medical

---

58. *Id.*

59. Jon Mills, *On Web, Families of Victims Entitled to Privacy*, U. FLA. NEWS (Mar. 2, 2010), https://news.ufl.edu/archive/2010/03/on-web-families-of-victims-entitled-to-privacy.html [https://perma.cc/PC5G-LY9E].

60. Catsouras v. Dep't Cal. Highway Patrol, 104 Cal. Rptr. 3d 352, 357-59 (Ct. App. 2010). However, Nikki Catsouras had not been drinking and a toxicology screening found a blood alcohol content of zero. R. Scott Moxley, *EX-CHP Employee Loses Again on Leak of Decapitation Pictures*, OC WKLY. (May 26, 2011), https://www.ocweekly.com/ex-chp-employee-loses-again-on-leak-of-decapitation-pictures-6460655/ [https://perma.cc/A6TE-W7YC].

61. Bennett, *supra* note 54.

62. *See* 381 U.S. 479, 485 (1965).

63. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 6521 cmt. b (AM. L. INST. 1977).

64. *See supra* note 41 and accompanying text.

65. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.) [hereinafter HIPAA].

66. 5 U.S.C. § 552.

treatment.[67] HIPAA is comprised of several overarching rules, including the Privacy Rule and the Security Rule.[68] HIPAA's Privacy Rule "governs the use and disclosure of protected health information"—information that identifies or can be used to identify an individual, an individual's health condition (past, present, or future), the healthcare an individual receives, as well as payment information.[69] In addition, HIPAA's Security Rule mandates "specific protections to safeguard" an individual's information when it is stored electronically.[70] One of the most important provisions in HIPAA creates an individual's right to control who sees her health information and how that information is used.[71] Except in instances where access to health information would affect an individual's care, the individual retains the power to control access and use of their health information.[72] While HIPAA limits an individual's absolute control over their health information, it does provide another protection for an individual's privacy: HIPAA prohibits the release of an individual's personal health information for fifty years following the individual's death.[73] The Department of Health and Human Services identifies the privacy interests of surviving relatives and the decedent's wishes as the main forces driving this protection.[74]

HIPAA has generally been read both as creating a floor rather than a ceiling in regulating personal health information and as allowing states to create more restrictive privacy schemes.[75] There

---

67. *See* Austin Rutherford, Comment, Byrne*: Closing the Gap Between HIPAA and Patient Privacy*, 53 SAN DIEGO L. REV. 201, 204 (2016).

68. *Your Rights Under HIPAA*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html [https://perma.cc/XAD8-DCEX].

69. Rutherford, *supra* note 67, at 204-05.

70. *Privacy, Security, and Electronic Health Records*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf [https://perma.cc/C8UM-GNEV].

71. *See Your Health Information Privacy Rights*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf [https://perma.cc/ED2U-AD2M].

72. *Id.*

73. *See* 45 C.F.R. § 160.103(2)(iv) (2018) (defining "protected health information").

74. *See Health Information of Deceased Individuals*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/ privacy/guidance/health-information-of-deceased-individuals/index.html [https://perma.cc/KEK6-JP3W].

75. Rutherford, *supra* note 67, at 206.

is a growing question of whether HIPAA creates a private right of action, particularly as the theft of personal health information through data breaches targeting healthcare companies appears to be on the rise.[76] In 2018, the Connecticut Supreme Court interpreted HIPAA as creating a private right of action when an individual sued a clinic for violating her HIPAA rights by disclosing her medical information to a third party without her knowledge or consent.[77] However, the consensus among the federal courts of appeal remains that HIPAA neither creates nor implies a private right of action.[78] The remaining remedies in HIPAA are fines against the violating entity, which still vindicate a patient's right to privacy.[79] It remains clear that Congress intended to protect posthumous privacy to personal health information and incorporated that intention in HIPAA's statutory framework.[80]

While the posthumous privacy interests encompassed by FOIA may be less easily intuited than in HIPAA, Congress and the courts have recognized and respected this interest since FOIA went into effect in 1967.[81] The overarching objective of FOIA is to provide "the public the right to request access to records from any federal agency."[82] Its purpose is to give "a broad right of access to 'official information'"[83] that enables the people to "know *what their government is up to*."[84] That access, however, is not unlimited, and several classes of exemptions preclude certain information from being

76. *See* Reed Abelson & Julie Creswell, *Data Breach at Anthem May Forecast a Trend*, N.Y. TIMES (Feb. 6, 2015), https://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html [https://perma.cc/76SP-UNZM].

77. *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 49 (Conn. 2014).

78. *See, e.g.*, Mayfield v. Presbyterian Hosp. Admin., 772 F. App'x 680, 686 (10th Cir. 2019) (holding that HIPAA does not create a private right of action); Bradley v. Pfizer, Inc., 440 F. App'x 805, 809-10 (11th Cir. 2011) (noting that there is no private right of action for a violation of HIPAA's confidentiality provisions); Miller v. Nichols, 586 F.3d 53, 59 (1st Cir. 2009) (holding that HIPAA does not create a private right of action).

79. *See* 45 C.F.R. § 160.402 (2018).

80. *See generally* HIPAA, *supra* note 65, § 264.

81. *FOIA Legislative History*, NAT'L SEC. ARCHIVE, https://nsarchive2.gwu.edu/nsa/foialeghistory/legistfoia.htm [https://perma.cc/2C8U-WNKR].

82. *What Is the FOIA?*, U.S. DEP'T JUST., https://www.foia.gov/faq.html [https://perma.cc/662J-3B8E].

83. U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 772 (1989) (quoting EPA v. Mink, 410 U.S. 73, 80 (1973)).

84. *Id.* at 773 (quoting *Mink*, 410 U.S. at 105).

released, most notably "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"[85] and "records or information compiled for law enforcement purposes ... [that] could reasonably be expected to constitute an unwarranted invasion of personal privacy."[86]

Courts have repeatedly granted FOIA exemptions when parties have requested death scene photographs, specifically citing Exemption 7(C)—the exemption focused on law enforcement records.[87] Because courts have been reluctant to read a right to privacy as extending beyond the grave, the first challenge in these FOIA requests is to identify whether there is a cognizable claim to privacy.[88] In *National Archives and Records Administration v. Favish*, regarding a FOIA request for death scene photographs of Deputy White House Counsel Vince Foster's suicide, the Court recognized that Foster's family had a cognizable right to privacy and extended Exemption 7(C) to the family.[89] Though the Court did not find that the family occupied the same position as the individual subjected to potential disclosure, it concluded that Congress "intended to permit family members to assert their own privacy rights against public intrusions long deemed impermissible under the common law and in our cultural traditions."[90] This connects a legal posthumous privacy interest with the cultural posthumous privacy interest discussed above, illustrating a shared sense of posthumous dignity and respect running throughout different considerations of the right to privacy.

85. 5 U.S.C. § 552(b)(6).

86. *Id.* § 552(b)(7).

87. *See* Nat'l Archives & Recs. Admin. v. Favish, 541 U.S. 157, 170 (2004); *see also* Campus Commc'ns, Inc. v. Earnhardt, 821 So. 2d 388, 392 (Fla. Dist. Ct. App. 2002) (providing background on a mediated settlement between the Earnhardt family and a newspaper seeking to publish autopsy photographs following Dale Earnhardt's fatal car crash in 2001).

88. As discussed in Part I.A, the dead cannot be defamed.

89. 541 U.S. at 160-61, 170.

90. *Id.* at 167.

II. THE RIGHT TO DATA PRIVACY

Before the digital revolution, most personal information existed solely in papers and documents.[91] The potential for unauthorized distribution of personal effects was rather limited,[92] and the decedent's heirs generally exercised near total control.[93] For example, the postal service could not read a decedent's mail or scan its contents.[94] In an increasingly digital and interconnected world, however, an individual's online footprint and digital trail can reveal virtually limitless information about an individual's physical and mental health,[95] biometric data,[96] social network, daily routine, taste in music and entertainment, and preferred news organizations.[97] The challenge this kind of information presents is not just in its sheer volume, but also in how seamlessly and quickly this data can be tied to an individual, packaged, sold, and distributed.[98]

As the Supreme Court has noted in several Fourth Amendment cases going all the way back to *Katz*, modern technology creates new challenges to reasonable expectations of privacy.[99] The pace of

---

91. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1172 (2002).

92. *See* Amitai Etzioni, *A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational*, 80 BROOK. L. REV. 1263, 1264 (2015) (noting that privacy violations in the paper age resulted predominantly from primary collection of the papers and that any secondary usage was limited).

93. *See* Lopez, *supra* note 22, at 192-93.

94. *See id.* at 218 (describing how email providers like Google and Yahoo scan their customers' emails for data to feed targeted marketing campaigns).

95. The health-related information collected by smart watches and fitness trackers now includes physical activity, the location of that activity, heart rate, metabolism, sleep cycles, blood sugar levels, and menstrual cycles. *See* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 426-27 (2018).

96. Biometric data includes facial scans and voice and finger prints. *See id.* at 427, 436.

97. *See* Riley v. California, 573 U.S. 373, 393-97 (2014) (discussing the various kinds of data and personal information an individual's cell phone may reveal).

98. *See* Kari Paul, *Fitness and Health Apps May Be Sharing the Most Personal Details About Your Life*, MARKETWATCH (Mar. 5, 2019, 7:47 AM), https://www.marketwatch.com/story/fitness-and-health-apps-may-be-sharing-the-most-private-details-about-your-life-2019-02-26 [https://perma.cc/46P3-9KNB].

99. Katz v. United States, 389 U.S. 347, 359 (1967) (establishing that Fourth Amendment protections "do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures"). Though

digital innovation continues to accelerate, while the law struggles to keep pace.[100] Consider, as one example, that there are no federal laws regulating the use of facial recognition software in law enforcement.[101] Ethicists have argued that, without regulation, facial recognition software could be linked to state and federal law enforcement databases, creating the following scenario: a police officer wearing a body camera and walking through a crowd of people would be able to instantaneously identify individuals with outstanding arrest warrants, those with expired visas, and even those with an expired driver's license.[102] Such a scenario chillingly evokes George Orwell's vision of a dystopian future society where Big Brother is always watching.[103]

Compounding these concerns of a sinister panopticon are two recent reports. First, the Federal Trade Commission recently found that there are literally billions of data elements collected and attached to nearly every American.[104] In November 2019, reporting revealed that Google's parent company (Alphabet) partnered with a nonprofit hospital organization on a data project intended to

---

a consideration of data privacy and personal information in the context of Fourth Amendment protections is beyond the horizon of this Note, there is considerable scholarship developing in the wake of the Supreme Court's ruling in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *See, e.g.*, Ryan G. Bishop, Note, *The Walls Have Ears ... and Eyes ... and Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667, 671 (2019) (arguing that smart home devices "have the potential to provide a pervasive and panoptic view of a person's daily life ... [and] implicate[] serious privacy concerns"); Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2211 (2019) (explaining how tracking cookies collect significant data about individuals without their knowledge).

100. *See* Tarry Singh, *AI Economy Will Further Accelerate the Pace of Innovation*, FORBES (Mar. 4, 2019, 10:28 AM), https://www.forbes.com/sites/cognitiveworld/2019/03/04/ai-economy-will-further-accelerate-the-pace-of-innovation/ [https://perma.cc/Z8UM-4GTZ].

101. *See* Sidsel Overgaard, *A Soccer Team in Denmark Is Using Facial Recognition to Stop Unruly Fans*, NPR (Oct. 21, 2019, 5:39 PM), https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans [https://perma.cc/5Q35-TCAJ].

102. *See* Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 1:19 AM), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/HPU8-S4TX].

103. *See generally* GEORGE ORWELL, 1984 (1949).

104. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at iv (2014).

enhance medical artificial intelligence.[105] With "Project Nightingale," Google now has access to tens of millions of patients' medical records through its partnership with healthcare provider Ascension—without the patients' consent.[106] Concerns about how Google will use this data and whether it is in compliance with applicable federal laws fall into an uneasy orbit around the search giant, which has already amassed data sets as wide and diverse as our email correspondence (Gmail), search history, shopping behavior, and biometric data (through its recent acquisition of Fitbit).[107]

Against this backdrop of the growing range of data sources, the integration of disparate sources, and the unknown potential of how they will be used, this Note now turns to consider the strongest legal frameworks to protect against the abuse of one's data and privacy.

A. The First Data Privacy Framework: GDPR

The first comprehensive legislation to address data privacy emerged from the European Union in 2016 and came into effect in May 2018: the General Data Protection Regulation (GDPR).[108] GDPR's overarching intent is to provide consumers with greater control over their personal data.[109] GDPR originates from an understanding of the "right to the protection of personal data" as one of an individual's "fundamental rights and freedoms."[110] GDPR gives individuals the right to discover what information a company keeps about them, how that information was collected, and how the information is being used.[111] It also empowers individuals to choose to be forgotten by corporations, effectively requiring data-collecting

105. *See* Sidney Fussell, *Google's Totally Creepy, Totally Legal Health-Data Harvesting*, THE ATLANTIC (Nov. 14, 2019), https://www.theatlantic.com/technology/archive/2019/11/google-project-nightingale-all-your-health-data/601999/ [https://perma.cc/8EYG-WVCR]. Google and Ascension both assert that the deal complies with HIPAA, but the Department of Health and Human Services has stated it wants to know more. *See id.*

106. *Id.* ("Neither affected patients nor Ascension doctors were made aware of the project.")

107. *See id.*

108. *See* Arjun Kharpal, *Everything You Need to Know About a New EU Data Law that Could Shake Up Big US Tech*, CNBC (May 25, 2018, 5:27 AM), https://www.cnbc.com/2018/03/30/gdpr-everything-you-need-to-know.html [https://perma.cc/PV49-KFDU].

109. *Id.*

110. 2016 O.J. (L 119) 32.

111. *See id.* at 43.

companies to delete the individual's information and to stop collecting the individual's information in the future.[112] Individuals can also halt third parties from using and selling their information.[113]

A key part of GDPR is consent.[114] Companies must clearly explain what they seek consumers' consent to, specifically what data they will collect from individuals.[115] Companies must also make it easy for consumers to revoke their consent at any time.[116] Under GDPR, only individuals older than sixteen may give consent.[117] Parents may give consent for their children under sixteen, but GDPR prohibits any data collection on children under thirteen.[118] By restricting the collection of data from and about children, GDPR addresses a major concern among privacy advocates.[119]

While GDPR regulates the actions of companies that operate within the EU and the European Collective Economic Bloc, it also protects the data privacy rights of all individuals living within the EU.[120] This requires U.S. companies to adhere to GDPR when interacting with individuals living in the EU.[121] However, it can be difficult to know with certainty when a consumer falls within GDPR protection. Because fines for noncompliance range up to 4 percent of the offending company's total global revenue, many companies with international consumer bases (or potential EU-based consumers) began adhering to GDPR when it went into effect.[122]

Ultimately, American consumers under this regime experienced the worst of both worlds. They were treated to annoying footers asking for consent to sites' cookie policies while receiving none of the protections granted to their EU-based brethren. However, the

---

112. *See id.* at 43-44.
113. *See id.* at 45.
114. *See id.* at 37.
115. *Id.* at 8.
116. *Id.* at 37.
117. *Id.*
118. *Id.*
119. For a discussion of minors' overarching right to privacy, see Helen L. Gilbert, Comment, *Minors' Constitutional Right to Informational Privacy*, 74 U. CHI. L. REV. 1375 (2007).
120. 2016 O.J. (L 119) 33.
121. *See id.*
122. Kharpal, *supra* note 108.

introduction of new legislation coming out of California could change all that.[123]

B. The American Solution: California Consumer Privacy Act

California has had a long tradition of blazing a path forward for the nation in watershed regulatory events. California has been the vanguard on key issues like climate change, when, "frustrated with inaction at the federal level ... [i]n 2002, California passed Assembly Bill 1493," which set the nation's first limits for greenhouse gas emissions produced by automobiles.[124] With an economy that represents 14 percent of the national economy, California often sets the bar for compliance in various industries through its enactment of key legislation; companies that do business in California likely do business nationwide.[125] The costs of maintaining multiple regulatory schemes often prove too high to manage, leaving corporations to adopt the most rigorous existing standards.[126]

Taking up the mantle of the nation's trailblazer, California began to seriously consider data privacy rights with the EU's consideration of GDPR.[127] As home to Silicon Valley and its myriad digital giants, California was uniquely positioned to address data privacy and to signal to the major industry players that they must begin to protect it.[128] Citing the increase in "the role of technology and data in the every daily [sic] lives of consumers,"[129] the "devastating effects" to consumers caused by unauthorized data disclosures and the

---

123. At the time of writing, no major news stories have been published on implementation and rollout of such legislation.

124. Jody Freeman, *The Obama Administration's National Auto Policy: Lessons from the "Car Deal,"* 35 HARV. ENV'T L. REV. 343, 349 (2011).

125. *See* Matthew A. Winkler, *The California Economy Isn't Just a U.S. Powerhouse*, BLOOMBERG (Apr. 24, 2019, 4:28 PM), https://www.bloomberg.com/opinion/articles/2019-04-24/california-economy-soars-above-u-k-france-and-italy [https://perma.cc/6NRK-SZJT]. California's economy is the fifth largest in the world, behind the U.S., China, Japan, and Germany. *See id.*

126. *See supra* Part II.A (discussing an analogous scenario in which GDPR sets a higher regulatory bar for foreign companies doing business in Europe).

127. Sarah Hospelhorn, *California Consumer Privacy Act (CCPA) vs. GDPR*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/ccpa-vs-gdpr/ [https://perma.cc/QD6H-W3CN] ("The CCPA is an outcome of the GDPR's reaching influence.").

128. *See* Winkler, *supra* note 125.

129. California Consumer Privacy Act of 2018, ch. 55, § 2(d), 2018 Cal. Stat. 1807, 1808-09.

"loss of privacy,"[130] and Cambridge Analytica's illicit use of tens of millions of consumers' data,[131] California created CCPA to ensure the following rights:

> (1) The right of Californians to know what personal information is being collected about them.
>
> (2) The right of Californians to know whether their personal information is sold or disclosed and to whom.
>
> (3) The right of Californians to say no to the sale of personal information.
>
> (4) The right of Californians to access their personal information.
>
> (5) The right of Californians to equal service and price, even if they exercise their privacy rights.[132]

In addition, CCPA provides extensive definitions of personal information,[133] which businesses are subject to regulation,[134] and what "selling" personal information means.[135] While CCPA can be broadly understood as a reaction to the misuse of consumers' digital personal information, the Act makes clear that CCPA encompasses all data that businesses collect about consumers, including their off-line behavior.[136]

While CCPA is primarily concerned with consumer privacy as a right in itself, it also implicitly acknowledges that control over one's personal information includes the ability to prevent corporations from monetizing one's personal information to create a profit.[137] The extensive definitions of business and commercial purposes, transfers, sales, and disclosures reveal CCPA's twin protections: the right to privacy and the right to remain an individual

130. *Id.* § 2(f).
131. *Id.* § 2(g).
132. *Id.* § 2(i).
133. CAL. CIV. CODE § 1798.140(o) (West 2020).
134. *See id.* § 1798.140(c).
135. *Id.* § 1798.140(f), (t).
136. *Id.* § 1798.175.
137. *See id.* § 1798.120(a).

and not a product.[138] CCPA protects businesses' ability to use personal data for improving products and services and debugging software.[139] However, it clearly empowers consumers to stop businesses from selling their personal information.[140] This is likely to have a significant impact on companies like Facebook, whose recent court filings show that the social media giant increased its revenue per user sevenfold after giving third-party developers access to consumers' personal information in exchange for a cut of the developers' revenue.[141] Where Facebook must comply with GDPR (and, thus, can be prevented from selling consumer data), its revenue per user is significantly less.[142]

Two important, related provisions of CCPA factor into the following analysis. First, CCPA allows an individual to exercise privacy rights on behalf of another individual, provided the latter has so authorized the former.[143] This is a broad right and extends beyond parents and guardians acting on behalf of their minor children, because CCPA addresses the sale of the personal information of minors separately.[144] One can imagine this provision being used by the guardians of vulnerable individuals or by the adult children of impaired parents. Part of the provision's intent appears to be making the right easy to use and understand. Underscoring this intent are other requirements for businesses, such as the posting of a link on a business's homepage to a web page where consumers may consent to, or opt out of, information collection.[145]

A second key provision of CCPA differentiates it from HIPAA and FOIA.[146] CCPA creates a private right of action for consumers to file civil suit when their data has been disclosed without their authorization or when businesses violate their personal

138. *See id.* § 1798.140(d), (f), (t).

139. *See id.* § 1798.105(d)(2)-(3).

140. *Id.* § 1798.120(a).

141. *See* Elena Botella, *Facebook Earns $132.80 from Your Data per Year*, SLATE (Nov. 15, 2019, 3:25 PM), https://slate.com/technology/2019/11/facebook-six4three-pikinis-lawsuit-emails-data.html [https://perma.cc/ZPR4-S6BD].

142. *Id.* In Europe, Facebook's average revenue per user is $41.91, compared with $132.80 in the United States. *Id.*

143. *See* CIV. § 1798.135(c).

144. *See id.* § 1798.120(d).

145. *Id.* § 1798.135(a)(1).

146. *See supra* Part I.C (discussing HIPAA and FOIA).

information collection preferences.[147] HIPAA, as discussed above, has been widely interpreted as barring private rights of action.[148] Under CCPA, this private right of action allows courts to award money damages (on a per-incident basis), declaratory and injunctive relief, or "[a]ny other relief the court deems proper."[149]

There is, however, one set of Californians that CCPA does not explicitly protect: the dead. Weaving together CCPA's private right of action and its provision allowing individuals to exercise privacy rights on behalf of others, this Note will explore how CCPA has created a clear direction on how to consider and protect posthumous data privacy rights.

III. THE DATA PRIVACY RIGHTS OF THE DEAD

Before embarking on an analysis of potential posthumous privacy frameworks, one might be forgiven for asking why the dead need data privacy. After all, the principles underlying the denial of posthumous defamation surely apply to posthumous privacy—the dead cannot be embarrassed.[150] The dead must be beyond caring whether someone discovers that they Googled personally embarrassing information.[151] The dead cannot be served extremely specific targeted ads online.[152] The dead are no longer affected by data breaches that release their personally identifiable information to the dark web.[153] Why devote any time or effort to such a purely academic exercise?

---

147. *See* CIV. § 1798.150(a).

148. *See supra* notes 75-80 and accompanying text.

149. CIV. § 1798.150(a)(1)(c).

150. Melissa Gaied, Note, *Data After Death: An Examination into Heirs' Access to a Decedent's Private Online Account*, 49 SUFFOLK U. L. REV. 281, 296 (2016).

151. For the living, however, the plethora of articles rounding up embarrassing Google searches by states illustrate that the concern is real. *See, e.g.*, Joe Berkowitz, *Infographic: Here Are the Most Embarrassing Popular Google Searches in Each State*, FAST CO. (Aug. 27, 2015), https://www.fastcompany.com/3050425/infographic-here-are-the-most-embarrassing-popular-google-searches-in-each-state [https://perma.cc/MUP5-CG7D].

152. *See* Zittrain, *supra* note 14.

153. *See, e.g.*, David Yaffe-Bellany, *Here's What You Need to Know About the Capital One Breach*, N.Y. TIMES (July 30, 2019), https://www.nytimes.com/2019/07/30/business/capital-one-breach.html [https://perma.cc/XFP9-DVAU].

Yet, as discussed above, there are instances in which American society does consider the dead's wishes and interests—even when such interests matter only to the living.[154] Laws require respect for a decedent's dignitary interests and prohibit desecration and other mistreatment of human remains—even though a decedent could never know.[155] Whether these laws actually aim to protect a decedent's heirs from emotional distress or to protect the decedent's dignitary interests, the outcome remains the same. Although the dead can never know whether they receive a burial in accordance with their wishes, American laws and culture dictate respect for a decedent's wishes, no matter whether those wishes are expressed in a will or by another manner.[156]

Similarly, these wishes can include expression of a wish for posthumous privacy, as in the case of the public figure who seals her papers for fifty years following her death.[157] In such a case, if a decedent expressed a desire for data privacy—particularly if this decedent were a Californian and fell under the protection of CCPA—the combination of customary respect for dying wishes and CCPA's protections would make a case for posthumous data privacy. CCPA even appears to accommodate this with its provision allowing a duly authorized individual to assert the privacy rights of another.[158] Whether CCPA would require a will or other documentation of this wish for posthumous data privacy is unclear, though the spirit of the legislation seems to favor a liberal construction of privacy rights.[159]

---

154. *See supra* Parts I.A, I.B.

155. *See supra* Parts I.A, I.B. The many ghost stories in American culture that start with a violation or desecration of a decedent's burial site, of which Stephen King's *Pet Sematary* is a notable example, speak to the strong cultural taboo against disregarding the dead's wishes. *See* STEPHEN KING, PET SEMATARY (1983).

156. *See supra* Parts I.A, I.B; *see also* Lithwick, *supra* note 35.

157. For example, T.S. Eliot's letters to an old flame were recently unsealed, fifty years after the deaths of both parties. Violet Kim, *T.S. Eliot Left a Deliciously Petty Note to Future Readers of His Private Letters*, SLATE (Jan. 2, 2020, 8:36 PM), https://slate.com/culture/2020/01/t-s-eliot-letters-emily-hale-princeton.html [https://perma.cc/4CQT-SEWX].

158. *See* CAL. CIV. CODE § 1798.135(c) (West 2020); *see also supra* notes 143-45 and accompanying text.

159. *See* CIV. § 1798.194 ("This title shall be liberally construed to effectuate its purposes."). For those decedents who did not express a desire for data privacy in life, the path forward is unclear. One might argue persuasively that these decedents should not enjoy rights in death that they did not proactively seek in life.

Given the recent emergence of data privacy as a concept, it follows that few have considered or articulated final wishes for the disposition of their data privacy. In the United States, with an average life expectancy of seventy-six years for men and eighty-one years for women[160] and rates of digital adoption that show an inverse relationship between age and internet usage,[161] this topic unsurprisingly has not been extensively explored in end-of-life planning. After all, if those who are statistically closest to death are generally unfamiliar with how their data is collected and used (an assumption made given their low rates of internet usage), it is plausible that those individuals may not express strong opinions on the use of their personal information after death. The individuals who are more likely to be aware of how their personal information is collected and used, following this line of reasoning, are more likely to be younger and, potentially, more likely to die intestate.[162] Therefore, the combination of data privacy protections heralded by CCPA and the strong likelihood that individuals will increasingly want to exercise these protections makes it very likely that discussions of posthumous data privacy will become part of end-of-life planning. The fight has already begun on another front, in which the untimely deaths of more digitally savvy individuals have resulted in legal battles with the digital giants over their heirs' ability to access digitally stored personal information, such as email accounts or social media profiles.[163]

One might reasonably ask, because GDPR so strongly influenced CCPA,[164] whether GDPR can provide guidance where CCPA has been silent. However, GDPR is also silent on whether privacy protections apply posthumously; in fact, "the GDPR does not provide any protection for data of deceased data subjects," and this silence "has triggered an interesting debate" among scholars in the

160. *Actuarial Life Table*, SOC. SEC. ADMIN. (2016), https://www.ssa.gov/oact/STATS/table4c6.html [https://perma.cc/UMJ4-HA8V].

161. *See Internet Use by Age*, PEW RSCH. CTR. (Jan. 11, 2017), https://www.pewresearch.org/internet/chart/internet-use-by-age/ [https://perma.cc/5BRP-HPC9] (showing that 100 percent of eighteen- to twenty-nine-year-old individuals and only 73 percent of individuals sixty-five and older are online).

162. *See* Natasha Chu, *Protecting Privacy After Death*, 13 NW. J. TECH. & INTELL. PROP. 255, 259-60 (2015).

163. *See id.* at 262-63; *see also* Ajemian v. Yahoo!, Inc., 84 N.E.3d 766, 768-70 (Mass. 2017).

164. *See* Hospelhorn, *supra* note 127.

international community.[165] GDPR allows EU member states to create their own legislative solutions for posthumous data privacy protections, resulting in at least four unique approaches from Estonia, Italy, France, and Catalonia.[166] Some of these frameworks conceive of personal information as a kind of "quasi-property," while another framework analogizes posthumous data privacy protection to a healthcare-advanced directive.[167]

While not following the various EU approaches precisely, this Note will now return to the three posthumous rights frameworks discussed in Part I, identify the key points of each approach, and weave these together to produce a proposal to create posthumous data privacy.

A. A Dignitary Approach

The dignitary rights framework stems from deeply held cultural beliefs in the importance of honoring and respecting the dead. One could argue the innate logic that requires laws to protect the bodies of the dead from insult and injury should also apply to the revealing search histories (and other personal information) of the departed.[168] Shielding the dead from indignity is an important aspect of respecting a decedent's wishes and protecting the heirs from unnecessary pain and suffering, as discussed above in the sad afterlife of images from Nikki Catsouras's car crash.[169] Dignitary laws act on behalf of both the decedent and the decedent's heirs.[170]

Arguably, however, an individual's search history—however embarrassing it may be—is unlikely to spring into a second life in a way that would attract public attention, particularly if the decedent is not otherwise known to the public. Though American society bridges ever-greater connections via memes and viral moments,

---

165. Gianclaudio Malgieri, *R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects Between Theoretical Scenarios and National Solutions*, *in* DATA PROTECTION AND PRIVACY: THE INTERNET OF BODIES 1, 2 n.1 (Ronald Leenes et al. eds., 2018).

166. *Id.* at 2, 12.

167. *See id.* at 2-3, 12-18.

168. *See supra* Part I.B.

169. *See supra* notes 54-61 and accompanying text.

170. *See* Lithwick, *supra* note 35.

the likelihood of any individual's personal information breaking through the growing digital noise is increasingly slight.[171] Indeed, some evidence suggests that American culture may be becoming more sensitive to the plight of those made viral against their wishes and more willing to protect the vulnerable from cyberbullying.[172] However, online communities have become increasingly adept at using social media and other platforms to publicly call out racism, homophobia, and other biases.[173] The criteria defining sympathetic victims are evermore blurry and shifting; ultimately, a decedent and their heirs cannot rely on cultural protections to ensure posthumous privacy.

However, one customary dignitary protection remains available for privacy: the sealing of one's personal papers.[174] While this most often occurs in the estates of individuals whose contributions to a society's cultural or academic life merit special consideration,[175] anyone can request that protection in a will or to an heir. The ability to seal records is the linchpin of the next privacy approach this Note will consider: HIPAA.

B. A HIPAA- and FOIA-Influenced Approach

For posthumous privacy, HIPAA's provisions constitute the clearest legal protections for an individual's personal information. Per 45 C.F.R. § 160.103, an individual's protected health information is protected for fifty years after death.[176] This protected

---

171. For a deeper dive into memes and how their growing use triggers interesting copyright and property rights questions, see Lauren Levinson, Comment, *Adapting Fair Use to Reflect Social Media Norms: A Joint Proposal*, 64 UCLA L. REV. 1038 (2017).

172. *See, e.g.*, Mendel Forta, Note, *Cyberbullying: Are You Protected? An Analysis and Guide to Effective and Constitutional Cyberbullying Protections*, 37 CARDOZO ARTS & ENT. L.J. 165, 185-87 (2019).

173. *See, e.g.*, Antonia Noori Farzan, *BBQ Becky, Permit Patty and Cornerstore Caroline: Too 'Cutesy' for Those White Women Calling Police on Black People?*, WASH. POST (Oct. 19, 2018, 6:08 AM), https://www.washingtonpost.com/news/morning-mix/wp/2018/10/19/bbq-becky-permit-patty-and-cornerstore-caroline-too-cutesy-for-those-white-women-calling-cops-on-blacks/ [https://perma.cc/SG6G-XPN7] (discussing the use of hashtags like #BBQBecky and videos to draw attention to the phenomenon of white women calling the police over the innocuous and entirely lawful activity of African Americans).

174. *See* Hodson, *supra* note 17, at 194-97; *see also* Kim, *supra* note 157.

175. *See* Hodson, *supra* note 17, at 202, 206.

176. *See* 45 C.F.R. § 160.103(2)(iv) (2018) (protected health information definition).

health information includes "demographic information collected from an individual,"[177] as well as personal information that

> (2) [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) [t]hat identifies the individual; or
>
> (ii) [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.[178]

This regulation appears to be the strongest protection for an individual's posthumous privacy in federal law.[179] Numerous concerns justify the protection of health information, including an innate respect for individual privacy and autonomy and a desire to protect individuals from discrimination based on an individual's health information.[180] In terms of posthumous privacy, however, only an innate respect for an individual's privacy explains the extension of protection to fifty years after the individual's death, when autonomy and discrimination are no longer viable concerns. Congress's perception of a need for posthumous privacy and motivation to create statutory protections for it highlight the importance of this interest.

One might argue, because HIPAA creates no private right of action for individuals or their heirs in the event of an unauthorized disclosure, HIPAA cannot be interpreted to support posthumous privacy. After all, there is no right without a remedy.[181] Yet, a textualist approach to statutory interpretation will underscore that including the fifty-year postmortem provision clearly expresses

---

177. *Id.* § 160.103 (individually identifiable health information definition).

178. *Id.* § 160.103(2)(i)-(ii) (individually identifiable health information definition).

179. This conclusion is based on a thorough (but not exhaustive) search of federal legislation.

180. For a discussion of "healthism," which is discrimination based on an individual's health condition(s), see Jennifer Bennett Shinall, *Intersectional Complications of Healthism*, 18 MARQ. BENEFITS & SOC. WELFARE L. REV. 255 (2017).

181. *L'ou le ley done chose, la ceo done remedie a vener a ceo*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("Where the law gives a right, it gives a remedy to recover.").

Congress's intent.[182] At the time of HIPAA's passage in 1996, hospitals and healthcare facilities were the primary creators and keepers of protected health information—Fitbit, 23andMe, and Apple would not come along for more than a decade to disrupt healthcare as powerful new players in personal health information.[183] The possibility of widescale data breaches and the unauthorized disclosure of protected health information posed a lower threat when HIPAA became law.[184] In light of this history, the limitations of hewing too closely to a traditional textualist interpretation come into sharp focus.

CCPA's own language closely parallels these definitions in HIPAA. HIPAA defines individually identifiable health information as information "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."[185] CCPA defines personal information, in part, as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[186] CCPA regulates the collection of IP addresses, devices, and data that would create a probabilistic basis for identification.[187]

CCPA addresses the concern that highly sophisticated actors can use seemingly innocuous data to create a profile to track an

---

182. *See, e.g.*, Richard H. Fallon, Jr., *Three Symmetries Between Textualist and Purposivist Theories of Statutory Interpretation—and the Irreducible Roles of Values and Judgment Within Both*, 99 CORNELL L. REV. 685, 687 (2014) (describing traditional textualism as being rooted in the notion "that the implications of statutory language are often unmistakable to any competent speaker of English, with no need for specialized knowledge about legal history or traditions").

183. Fitbit was founded in 2007. *Who We Are*, FITBIT, https://www.fitbit.com/us/about-us [https://perma.cc/U96E-2HGK]. 23andMe was founded in 2006. *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ [https://perma.cc/6QXP-QPVG]. And Apple debuted its Apple Watch in 2014. *Apple Unveils Apple Watch—Apple's Most Personal Device Ever*, APPLE (Sept. 9, 2014), https://www.apple.com/newsroom/2014/09/09Apple-Unveils-Apple-Watch-Apples-Most-Personal-Device-Ever/ [https://perma.cc/4JF8-DLL4].

184. *See, e.g.*, Lily Hay Newman, *The WIRED Guide to Data Breaches*, WIRED (Dec. 7, 2018, 9:00 AM), https://www.wired.com/story/wired-guide-to-data-breaches/ [https://perma.cc/659F-CGSU]. Although data breaches occurred prior to the digital revolution, their ubiquity and impact became greater with the advent of the internet. *See id.*

185. 45 C.F.R. § 160.103(2)(ii) (2018) (individually identifiable health information definition).

186. CAL. CIV. CODE § 1798.140(o)(1) (West 2020).

187. *See id.* § 1798.140(x).

individual across the internet, essentially creating a homing beacon that traces their movements from the moment they go online.[188] Similarly, apprehension of the unknown uses of personal information appears to drive the posthumous protection of health information. Though the utility of knowing that an elderly relative had her gallbladder removed seems just as unclear as the value of the departed's search history, such provisions in CCPA safeguard highly sensitive personal information from being used in unanticipated ways that are irreconcilable with a decedent's wishes and beliefs.

One must also note that HIPAA's posthumous protection has a shelf life of fifty years.[189] Such data is not destroyed, but merely taken out of reach for the time period when its relevance is highest.[190] Applying a similar hold and an expiration date to data privacy would harmonize with HIPAA's underlying concerns and would be consistent with the strongest current statutory protections of posthumous privacy. This approach would be an intentional departure from the time windows specified for data privacy in CCPA, which require individuals to renew their request for privacy every twelve months.[191]

Given the interest in finality when settling a decedent's estate, adopting a set privacy window feels more fitting in the posthumous context than requiring that the heirs repeatedly take action. There are very limited (and perhaps no) examples of estate administration that would require cyclical, repetitive actions to accomplish a single, overarching goal. The concerns attendant in administering an estate also inhere in the property-rights framework this Note turns to next.

C. A Property- and Publicity-Rights-Influenced Approach

While courts continue to consider whether intentionally created digital assets constitute property, neither courts nor legislatures have clearly determined whether the information created by an

188. *See supra* notes 129-39 and accompanying text.
189. *See* 45 C.F.R. § 160.103(2)(iv) (2020) (protected health information).
190. *See Health Information of Deceased Individuals*, *supra* note 74.
191. *See* CIV. § 1798.135(a)(5).

individual's online activities is property.[192] While CCPA addresses this kind of personal information, it does so from a privacy-rights framework.[193]

Analogizing this kind of personal information to property is not intuitive in part because, unlike intellectual property (another form of intangible property),[194] an individual creates this information unintentionally and unknowingly.[195] However, this intangible, unintentionally created data represents significant value to corporations (and governments) that can aggregate and mine the data.[196] This information begins to look like a kind of property due to its potential value and unclear ownership.

Establishing control over a potentially valuable and intangible form of property fits within the realm of publicity rights. In life, an individual exercises control over intangible assets like their image, likeness, and the uses of it.[197] In some states, an individual's family may continue to exercise publicity rights on behalf of the decedent.[198] For example, the estate of Elvis Presley has made a cottage industry of asserting vigorous control over the use of the King's likeness.[199] Typically, publicity rights have been limited to celebrities; however, there is no bright-line test to determine whether publicity rights are a viable cause of action for a decedent's heirs.[200] The appeal of the publicity-rights approach is that it can accommodate information unknowingly collected from an individual (say, a photograph), while also addressing the monetary value of such uses.

---

192. *See* Lopez, *supra* note 22, at 215.

193. *See* California Consumer Privacy Act of 2018, ch. 55, § 2(a)-(b), 2018 Cal. Stat. 1807, 1808.

194. The law recognizes many forms of intangible property. *See, e.g.*, RESTATEMENT (THIRD) OF PROP.: WILLS AND DONATIVE TRANSFERS § 6.2(h) (AM. L. INST. 2003); RESTATEMENT (FIRST) OF PROP. ch. 13, topic 2 (AM. L. INST. 1936).

195. However, the law acknowledges the existence of property in cases in which an individual dies intestate (that is, without expressing intent or even an awareness of the property in her estate) and provides for the estate's succession to the nearest heir. *See Intestate*, BLACK'S LAW DICTIONARY (11th ed. 2019). CCPA also includes information that businesses attach to individuals to trace them—unique identifiers such as "cookies, beacons, pixel tags, [and] mobile ad identifiers." CIV. § 1798.140(x).

196. *See* de Zayas, *supra* note 99, at 2211-12.

197. *See* Binder, *supra* note 37, at 299.

198. *Id.*

199. *Id.* at 297-98 n.4.

200. *Id.* at 299.

Yet, the theory of publicity rights on its own does not fully fit the contours of posthumous data privacy. On average, the amount of revenue an individual's personal information would create for a single corporation or industry does not approach what pirating the King's likeness represents for the Presley estate.[201] The scale of an individual's posthumous data privacy is significantly smaller than Elvis's estate, but taken in the aggregate, posthumous data privacy is massive. Indeed, about 90 percent of American adults use the internet,[202] and approximately 2.8 million Americans died in 2017.[203] In addition, while publicity rights typically apply only to the famous,[204] posthumous privacy must necessarily apply to all.

A better model to capture the individual economic value and the potential scope of data collection derives from the legacy of Henrietta Lacks.[205] In 1951, Henrietta Lacks, an African American woman living in Baltimore, was treated at Johns Hopkins for an aggressive form of cervical cancer that ultimately took her life.[206] During her diagnosis and treatment, researchers at the hospital took tissue from Lacks without her consent and made an amazing discovery—her cancer cells were immortal.[207] If fed with proper nutrition and kept in ideal conditions, these cells would reproduce infinitely.[208] The discovery of the first line of "immortal human cells"[209] transformed medicine, revolutionizing fields like virology[210] and human genetics.[211] Lacks's cells, known as HeLa cells,[212] were used to develop the polio vaccine[213] and in vitro fertilization, among

201. According to Forbes, the estate of Elvis Presley earned $35 million in 2017. Zack O'Malley Greenberg, *Elvis Presley's Earnings: $35 Million in 2017*, FORBES (Oct. 30, 2017, 12:51 PM), https://www.forbes.com/sites/zackomalleygreenburg/2017/10/30/elvis-presleys-earnings-35-million-in-2017 [https://perma.cc/P9TH-6G6C].

202. *Internet/Broadband Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/ [https://perma.cc/FQT8-HUWD].

203. *See* Kenneth D. Kochanek, Sherry L. Murphy, Jiaquan Xu & Elizabeth Arias, *Deaths: Final Data for 2017*, 68 NAT'L VITAL STAT. REP. 1, 1 (2019).

204. *See* Binder, *supra* note 37, at 299.

205. *See generally* REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS (2010).

206. *See id.* at 13, 86, 209.

207. *See id.* at 33, 41.

208. *See id.* at 41.

209. *See id.* at 1.

210. *Id.* at 98.

211. *Id.* at 100.

212. *See id.* at 1.

213. *See id.* at 93-97.

other breakthroughs.[214] Henrietta Lacks's cells created a new industry that sells human biological materials and generates significant revenue each year.[215] Yet, all this occurred without Henrietta Lacks's consent and without the knowledge of her heirs.[216] When published, the story of Henrietta Lacks caused an outcry and sparked a debate over the legal rights of individuals and their survivors.[217]

Lacks's story introduces an ethical dimension to this analysis that traces a new contour in the data privacy model. The unethical harvesting of HeLa cells was the first link in a long chain of events, each of which created corporate wealth and was tainted by that first ethical breach.[218] Similarly, when corporations harvest individuals' data without their knowledge or meaningful consent, it can feel like a (smaller-scale) ethical violation. The monetization of that data further exacerbates the ethical violation. In an apt parallel, Lacks's historian noted that today any one individual's cells are unlikely to spark the kind of medical revolution and corporate financial windfall HeLa cells did, just as any one individual's data is unlikely to create the next Silicon Valley billion-dollar start-up—instead, the value of an individual's cells comes from being part of a larger connection.[219] Similarly, the aggregation of individuals' data is how Facebook makes a killing.[220]

CCPA recognizes the potential for unethical corporate behavior and provides a resolution that puts California residents in control of their personal information.[221] Yet, the potential for unethical uses of personal information actually increases after an individual's death under the current law because corporations face no restrictions in the data of the dead. Recognizing and protecting the right to posthumous data privacy would close this key gap in the current legislation.

---

214. *Id.* at 2.

215. *See id.* at 194.

216. *See id.* at 6, 33.

217. *See generally* Gail Javitt, *Why Not Take All of Me? Reflections on* The Immortal Life of Henrietta Lacks *and the Status of Participants in Research Using Human Specimens*, 11 MINN. J.L. SCI. & TECH. 713 (2010) (presenting the central concerns in this bioethics debate).

218. *See* SKLOOT, *supra* note 205, at 194.

219. *Id.* at 322.

220. *See* Botella, *supra* note 141.

221. *See supra* notes 129-39 and accompanying text.

D. The Proposed Approach

This Note argues that a right to posthumous data privacy is the logical extension of several legal frameworks that already protect the rights of the dead, though no single framework fully traces the contours of this right. It is necessary, then, to weave together the protections from each framework to create a stronger and fully realizable posthumous data privacy right. First, creating a right to posthumous data privacy accords with the cultural respect for posthumous dignity discussed above.[222] Second, current statutes already provide two key aspects to posthumous data privacy protection, for instance, in HIPAA: the automatic sealing of personal health information and the fifty-year horizon under which the personal information remains under seal.[223] This is critical because HIPAA does not require that the decedent make an express wish for the privacy of their health information. Third, property and publicity rights provide an economic rationale for the need to protect posthumous data privacy.[224] Simply put, corporate revenue models are based on the use of individual data, even if an individual's data becomes valuable only when aggregated with that of other similar individuals.[225] There is also the underlying ethical requirement, articulated in CCPA, that individuals must have control over the use of their personal information.[226] The importance of that ethical requirement extends beyond death, as the case of Henrietta Lacks so elegantly illustrates.[227]

Some may question the extent to which posthumous protection should reach and whether all types of data should be protected equally. While some types of data may more directly implicate traditional privacy interests, there are at least two arguments against a tiered approach to posthumous data privacy. First, given the clear analogy between posthumous data privacy and HIPAA, HIPAA's approach should govern.[228] HIPAA does not create tiers

222. *See supra* Part I.A.
223. *See supra* notes 67-74 and accompanying text.
224. *See supra* Part III.C.
225. *See* Botella, *supra* note 141.
226. *See supra* notes 137-40 and accompanying text.
227. *See supra* notes 205-17 and accompanying text.
228. *See supra* Part III.B.

of posthumous health data protection, therefore neither should posthumous data privacy.[229] The second argument against tiering posthumous data privacy is the ease of implementation and enforcement. Neither GDPR nor CCPA tiers protection for data privacy. Introducing tiers of protection for posthumous data would complicate the regulatory schemes, make integration ungainly, and sow confusion within the affected industries.

California is uniquely positioned to break new ground in creating a posthumous data privacy right.[230] As the above analysis has argued, the legal and ideological foundation supporting data privacy rights also supports posthumous data privacy.[231] Change must come in the form of an amendment to CCPA that creates a right to posthumous data privacy and establishes a fifty-year seal on the release and use of data belonging to deceased Californians. The state's political landscape should facilitate the smooth integration of posthumous rights to data privacy. The political factors weighing in favor of the amendment's introduction and passage include CCPA's broad public approval,[232] CCPA's unanimous passage in 2018,[233] the Democratic Party's supermajority in both chambers of the California State Legislature,[234] a Democratic governor (Gavin Newsom),[235] and a Democratic attorney general (Xavier Becerra).[236] Since only state legislators may introduce bills in the legislature, Attorney General Becerra's office should work with the original bill's sponsors (Assemblyman Ed Chau and Senator Robert Hertzberg) to craft the amendment.[237] In the meantime, as the amendment makes

229. *See* 45 C.F.R. § 160.103(1)-(2) (2018) (protected health information definition).

230. *See supra* notes 124-26 and accompanying text.

231. *See supra* Part III.A-C.

232. *See* Kagan, *supra* note 6.

233. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ [https://perma.cc/M2NJ-Q5J8].

234. Patrick McGreevy, *Democrats Win Back a Supermajority in California's Legislature*, L.A. TIMES (Nov. 12, 2018, 9:15 PM), https://www.latimes.com/politics/la-pol-ca-democrats-supermajority-california-legislature-20181112-story.html [https://perma.cc/43W6-PAQ6].

235. *See id.*

236. *See* Cyrus Farivar & David Ingram, *California Is Bringing Law and Order to Big Data. It Could Change the Internet in the U.S.*, NBC NEWS (May 13, 2019, 11:47 AM), https://www.nbcnews.com/tech/tech-news/california-bringing-law-order-big-data-it-could-change-internet-n1005061 [https://perma.cc/6F9R-HBJW].

237. *See* Lapowsky, *supra* note 233.

its way through both legislative chambers, Attorney General Becerra should announce his support of posthumous data privacy and work with industry trade groups and industry leaders (like Facebook and Google) to prepare for compliance. A multi-industry advisory board that includes companies with HIPAA experience would also help the tech industry prepare for the amendment's passage. Passing an amendment and partnering with industry leaders would set the bar for future data privacy legislation coming out of other states, as well as for a federal raft of statutory protections.

CONCLUSION

The need to establish a right to data privacy is a product of the digital age, but the need to extend that right to the dead stems from a much older legal tradition, reaching back to the ancient Greeks moved by the tragedy of *Antigone*.[238] The right to dignity and respect after death exists just as much now in the modern United States as three thousand years ago in ancient Greece. Enshrining posthumous data privacy as a right honors the cultural heritage of American society's deeply held beliefs and takes into account the modern innovations of the technological age.

Kate C. Ashley[*]

238. *See supra* note 44 and accompanying text.

* J.D. Candidate, 2021, William & Mary Law School; M.B.A., 2008, Virginia Commonwealth University; M.A., English Literature, 2004, University of Washington; B.A., English Literature, 2001, University of Virginia. Thank you to Professor Neal Devins for his helpful advice and to Davis McKinney for his support and thoughtful comments throughout. Thank you to the *Law Review* student and professional staff for their hard work editing this Note and Volume.