Data After Death: An Examination into Heirs' Access to a Decedent's Private Online Account

"The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect . . . . They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[1]

I. INTRODUCTION

In the Internet age, protecting the privacy interests of individuals who predecease their digital accounts has resulted in ongoing legal uncertainty.[2] Much of the ambiguity stems from inconsistent regulation of digital privacy by federal and state governments, as well as private entities.[3] On one hand, federal law prohibits Internet service providers from disclosing content without owner consent or government order.[4] On the other hand, state judges grant court orders to grieving families, demanding that service providers, such as Facebook and Yahoo!, allow access to the decedent's account.[5] Providers then argue that such disclosure orders constitute a breach of contract because of preexisting privacy terms between the user and the provider.[6]

Further complicating the matter, some states have adopted legislation

1. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (urging courts to recognize common law right to privacy).

2. *See* Jeff Mordock, *Does Delaware's New Digital Asset Law Conflict with Federal Statute?*, DEL. L. WKLY. (Sept. 3, 2014), http://www.delawarelawweekly.com/id=1202668686577/Does-Delawares-New-Digital-Asset-Law-Conflict-With-Federal-Statute [https://perma.cc/9GFU-76MQ] (arguing conflicting regulations of online data after death results in legal uncertainty).

3. *See* Zach Miners, *Yahoo Slams New 'Digital Will' Law, Says Users Have Privacy When They Die*, NETWORK WORLD (Sept. 15, 2014), http://www.networkworld.com/article/2683473/yahoo-slams-new-digital-will-law-says-users-have-privacy-when-they-die.html [http://perma.cc/ZVA6-UXGS] (discussing Yahoo!'s criticism of expanded access into user accounts as violating initial user-provider agreement).

4. *See* Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2522 (2012) (protecting transmitted communications); *see also* Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712 (2012) (protecting electronically stored communications).

5. *See* John Conner, Comment, *Digital Life After Death: The Issue of Planning for a Person's Digital Assets After Death*, 3 EST. PLAN. & COMMUNITY PROP. L.J. 301, 301 (2011) (stating Michigan court granted family access to email account of son killed in military action).

6. *See* Molly Wilkens, Note, *Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?*, 62 HASTINGS L.J. 1037, 1053-54 (2011) (stating online providers take cautionary measures in protecting user privacy after death).

allowing a decedent's digital content to pass to his or her heir upon death—similar to the treatment of personal property.[7] Delaware recently enacted the most sweeping legislation, granting family members, executors, and heirs total control over the decedent's digital accounts—including email, social media, and cloud storage—the same way it grants rights over physical documents.[8] Despite such legislation, web-providers continue to remain reluctant to disclose user content to grieving families.[9]

In light of conflicting regulations, the right to privacy may, in fact, evolve as a posthumous right, similar to the evolution of the right to publicity and copyright.[10] Although the event of death deprives a person of his or her privacy right, such deprivation becomes exceedingly difficult to defend in the context of personal online data because such data is immortal by nature.[11] The Supreme Court acknowledged that digital content triggers greater privacy concerns due to the qualitative and quantitative nature of digital data.[12] Nonetheless, American law, in comparison to other developed countries, does not traditionally value the dignity of the dead.[13]

To understand the state of the controversy, this Note will begin with a historical discussion of the constitutional right to privacy and its evolution as it relates to digital privacy.[14] Further, this Note will discuss how federal, state, and private actors regulate digital privacy and this Note will posit that a discrepancy exists among such regulations.[15] This Note will then discuss how diverging regulations might trigger a debate in favor of a posthumous right to privacy, especially due to the lack of uniform regulation by federal, state, and

7. *See* Nicole Schneider, *Social Media Wills—Protecting Digital Assets*, 82 J. KAN. B. ASS'N 16, 16 (2013) (indicating states' adoption of digital asset laws). Connecticut, Rhode Island, Oklahoma, Indiana, and Idaho have adopted laws deeming digital assets as part of an estate. *See id*.

8. *See* DEL. CODE ANN. tit. 12, § 5004 (West 2015) (granting fiduciary control over decedent's digital data); *see also* Jacob Gershman, *Delaware Eases Access to Digital Data of Dead*, WALL ST. J. (Aug. 20, 2014), http://www.wsj.com/articles/delaware-eases-access-to-digital-data-of-dead-1408586848 (stating Delaware law allows fiduciaries more access and control of decedent's online account).

9. *See* Miners, *supra* note 3 (discussing Yahoo!'s criticism of executors' broad access to decedents' online accounts).

10. *See* RAY M. MADOFF, IMMORTALITY AND THE LAW: THE RISING POWER OF THE AMERICAN DEAD 6-7 (2010) (discussing evolution of copyright and right of publicity into posthumous rights).

11. *See* Schuyler v. Curtis, 42 N.E. 22, 25 (N.Y. 1895) (stating right of privacy possessed during life dies with person).

12. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (acknowledging digital data triggers greater privacy concerns). The Court stated, "Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Id*. Cell phones, however, store sixteen gigabytes of information, which equals millions of text pages, thousands of pictures, or hundreds of videos. *See id.* "The storage capacity of cell phones has several interrelated consequences of privacy." *Id*.

13. *See* MADOFF, *supra* note 10, at 7 (comparing American and European values of privacy and dignity of deceased). Unlike the United States, some European countries employ governmental entities to protect a person's privacy and reputational interests after death. *See id*.

14. *See infra* Part II.A.

15. *See infra* Part II.B.

private actors.[16] The Analysis section will examine the evolution of copyright and the right of publicity into posthumous rights and the strategic use of such doctrines to preserve privacy after death.[17] Finally, this Note will conclude with considerations of the future of a posthumous privacy right.[18]

II. HISTORY

A. The Right to Privacy and Its Dimensions

1. Origins of the Constitutional Right to Privacy

In *Griswold v. Connecticut*,[19] the United States Supreme Court first recognized the right of marital privacy as a constitutional right protected from governmental infringement.[20] The Court reached its holding by reasoning that the right of privacy in marriage is a fundamental right that the Constitution guarantees.[21] The Court subsequently expanded privacy rights to unmarried individuals in *Eisenstadt v. Baird*,[22] stating that the right to privacy adheres not in the marital couple but rather in the individual.[23] Further, in *Carey v. Population Services International*,[24] the Supreme Court expanded privacy rights to protect minors as well.[25] Through many precedential decisions, the Court recognized a constitutional guarantee of certain "zones of privacy," which encompasses personal decisions related to marriage, procreation, contraception, family relationships, child rearing, and education.[26]

16. *See infra* Part II.C.

17. *See infra* Part III.A.1.

18. *See infra* Part IV.

19. 381 U.S. 479 (1965).

20. *See id.* at 487 (Goldberg, J., concurring) (concluding marital privacy guaranteed as constitutional right).

21. *See id.* at 485 (majority opinion) (explaining right of privacy as legitimate constitutional right). The Court described marriage as "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees." *Id.* The Court further stated the Constitution "protects those liberties that are 'so rooted in the traditions and conscience of our people as to be ranked as fundamental.'" *Id.* at 487 (Goldberg, J., concurring) (quoting Snyder v. Massachusetts, 291 U.S. 97, 105 (1934)).

22. 405 U.S. 438 (1972).

23. *See id.* at 453 (holding right of privacy for individual regardless of marital status). Although the Court acknowledged *Griswold* merely questioned the right of marital privacy, it argued, "If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person." *Id.*

24. 431 U.S. 678 (1977).

25. *See id.* at 693 (extending privacy rights to minors, particularly in privacy decisions related to procreation).

26. *See id.* at 684-85 (recognizing Constitution's implicit protection of liberties under Fourteenth Amendment Due Process Clause); *see also* Roe v. Wade, 410 U.S. 113, 155 (1973) (determining governmental infringement upon fundamental right justified if narrowly tailored to serve compelling state interest).

2. Reasonable Expectation of Privacy Under the Fourth Amendment

a. Katz *Expectation-of-Privacy Test*

In *Katz v. United States*,[27] the Court analyzed privacy in a search and seizure context under the Fourth Amendment.[28] The Court ultimately held that when an individual enters a public telephone booth and makes a phone call, the government cannot record what that individual says without a warrant.[29] Justice Harlan concurred that the Court's reasoning emerged from precedent, invoking a "twofold requirement"—first, that the individual actually exhibits an expectation of privacy, and second, that the expectation is one society would consider reasonable.[30] Additionally, Justice Harlan agreed with the majority that the *Katz* holding would undoubtedly overrule *Goldman v. United States*,[31] where the Court held electronic surveillance without physically penetrating a target's premises did not violate the Fourth Amendment.[32] Justice Harlan further characterized the *Goldman* holding as "in the present day, bad physics as well as bad law" because electronic invasion, like physical invasion, could defeat reasonable expectations of privacy.[33]

b. Expectation-of-Privacy Test and Equilibrium-Adjustment Theory in Response to New Technologies Post Katz

In *United States v. Jones*,[34] the Court recognized the potential difficulties of applying the *Katz* expectation-of-privacy test, particularly in a society of ever-changing technology.[35] The Court stated it is difficult to apply the *Katz* test when an individual's privacy expectations might consistently and reasonably change in response to new technology.[36] New expectations would either cause

27. 389 U.S. 347 (1967).

28. *See id.* at 350 (stating Fourth Amendment protects individual privacy from certain governmental intrusions); *see also* U.S. CONST. amend. IV (protecting individuals from unreasonable searches and seizures).

29. *See Katz*, 389 U.S. at 359 (holding search and seizure by electronic surveillance violates Fourth Amendment absent procedural justification).

30. *Id.* at 361 (Harlan, J., concurring) (explaining Fourth Amendment rationalization does not extend to public acts).

31. 316 U.S. 129 (1942), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

32. *See id.* at 135 (reasoning use of detectaphone did not violate Fourth Amendment); *see also Katz*, 389 U.S. at 362 (Harlan, J., concurring) (noting *Goldman* should be overruled because electronic surveillance can violate Fourth Amendment).

33. *Katz*, 389 U.S. at 362; *see also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 22 (2004) (characterizing *Goldman* Court's requirement for surveillance physically penetrating target's premises as "silly technicality").

34. 132 S. Ct. 945 (2012).

35. *See id.* at 962 (Alito, J., concurring) (discussing difficulty in applying *Katz* test in technological era to determine individual's privacy expectations).

36. *See id.* (acknowledging difficulty of applying *Katz* test in digital era). The Fourth Amendment

the forfeiture of privacy or create concern over new intrusions of privacy.[37] The Court nonetheless analyzed the government's installation and use of a GPS tracking device on a person's vehicle under the *Katz* test, and it subsequently held such surveillance constituted a search and seizure requiring a warrant.[38]

More recently, in *Riley v. California*,[39] the Court held that law enforcement agencies could not, without a warrant, search digital information on an arrestee's cell phone; otherwise, such search would violate the individual's privacy rights.[40] The Court essentially applied Fourth Amendment protection in an era of new technology while noting that the onslaught of people carrying digital data substantially increases privacy concerns.[41] In reaching its decision, the Court considered the unique qualitative and quantitative nature of digital devices, categorizing cell phones as "minicomputers" with "immense storage capacit[ies]."[42] The Court acknowledged that unreasonable search and seizure of devices with such digitization capabilities had many privacy consequences.[43]

demands that courts not only monitor the effects of new technology on privacy, but also promulgate rules that reasonably regulate law enforcement agencies while protecting privacy as technology evolves. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 804-05 (2004).

37. *See Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (discussing consequences of new privacy expectations).

38. *See id.* at 954 (Sotomayor, J., concurring) (explaining government invaded protected privacy interest by "usurp[ing]" property to survey individual).

39. 134 S. Ct. 2473 (2014).

40. *See id.* at 2485 (declining to extend warrantless searches of cell phone data on lawfully arrested person). In *Riley*, the Court noted that although an arrest may reduce the arrestee's expectations of privacy, when concerns over privacy are significant, the law might nonetheless require a warrant to search the arrestee. *See id.* at 2488; *see also* Maryland v. King, 133 S. Ct. 1958, 1979 (2013) (stating warrant required to search arrestee when "privacy-related concerns are weighty enough").

41. *See Riley*, 134 S. Ct. at 2489-90 (distinguishing physical items from items holding digital data when deciphering intrusion of arrestee's privacy). The *Riley* decision set the precedent for applying Fourth Amendment protection in an era of digital technology:

> [T]he Court refused simply to extend to this new technology the exception to the Fourth Amendment's general requirement of a warrant based on probable cause that had been developed in a pre-digital era. It instead examined the practical, real-world intrusion on long-standing legitimate privacy expectations that would result from taking that step and, finding a significant intrusion, held that the warrant requirement, rather than the less-protective standard developed for the pre-digital environment, should apply.

Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2014 CATO SUP. CT. REV. 307, 308 (2014).

42. *Riley*, 134 S. Ct. at 2489. The Court explained that the unreasonable search and seizure of cell phones implicates extensive privacy concerns compared to the search of pocket items, such as a pack of cigarettes, a wallet, or a purse. *See id.* at 2488-89; *see also* Pincus, *supra* note 41, at 323-26 (discussing *Riley* Court's distinct consideration of cell phones' digital storage capabilities).

43. *See Riley*, 134 S. Ct. at 2489 (acknowledging digitized data triggers privacy concerns). Justice Alito argued that modern surveillance devices allow cheap and easy monitoring of an individual, in comparison to the costly traditional surveillance techniques of the precomputer era. *See* United States v. Jones, 132 S. Ct. 945, 963-64 (2012) (Alito, J., concurring).

Ultimately, the *Riley* Court applied an equilibrium-adjustment theory after recognizing that the government could attain evidence more readily because of new technology.[44] As a "correction mechanism," judges utilize the equilibrium method to embrace greater Fourth Amendment protections in the face of changing technology, while also maintaining the original degree of privacy protection that the Amendment guarantees.[45]

3. Survivor Privacy

Although the Constitution guarantees and protects an individual's right to privacy, it deprives the individual of that right upon his or her death.[46] The privacy rights of the surviving family members of the deceased, however, are preserved despite their loved one's death.[47] In *National Archives and Records Administration v. Favish*,[48] a media skeptic filed a Freedom of Information Act (FOIA) action, seeking to compel production of death-scene photographs of President Clinton's deputy counsel, who died of apparent suicide.[49] The FOIA, however, excuses disclosure of any information gathered for law enforcement purposes if one could reasonably expect its production would be an unwarranted invasion of personal privacy.[50] In interpreting the FOIA exemption, the Court concluded Congress intended the phrase "personal privacy" to allow family members of the deceased to assert their privacy rights

44. *See* Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 NW. U. L. REV. ONLINE 56, 61 (2014) (noting *Riley* Court's apparent but not explicit equilibrium analysis); *see also Riley*, 134 S. Ct. at 2490 (describing items carried prior to digital age as typically containing less sensitive personal information); Orin Kerr, *The Significance of* Riley, WASH. POST (June 25, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/ [http://perma.cc/772W-4J7J] (arguing *Riley* Court implicitly applied equilibrium-adjustment methodology).

45. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

46. *See* Schuyler v. Curtis, 42 N.E. 22, 25 (N.Y. 1895) (stating individual's right of privacy expires at death). The court further argued that the only surviving, thereby enforceable, privacy right was that of the decedent's surviving relatives. *See id.*; *see also* Roe v. Wade, 410 U.S. 113, 158 (1973) (arguing constitutional meaning of "person" does not include unborn); Catherine Leibowitz, Note, *"A Right To Be Spared Unhappiness": Images of Death and the Expansion of the Relational Right of Privacy*, 32 CARDOZO ARTS & ENT. L.J. 347, 350 (2013) (describing postmortem right of privacy as nonexistent).

47. *See Schuyler*, 42 N.E. at 25 (explaining survivor privacy rights). The right of privacy "exists for the benefit of the living, to protect their feelings and to prevent a violation of their own rights in the character and memory of the deceased." *Id.*

48. 541 U.S. 157 (2004).

49. *See id.* at 161; *see also* Barry Sullivan, *FOIA and the First Amendment: Representative Democracy and the People's Elusive "Right To Know,"* 72 MD. L. REV. 1, 63-67 (2012) (explaining history and objective of FOIA). The objective of the FOIA was to require public disclosure from the government, excluding cases where the government could demonstrate that a specific provision of the Act exempted disclosure. *See* Sullivan, *supra*, at 66.

50. *See Favish*, 541 U.S. at 160 (indicating FOIA exemption of public disclosure of records); *see also* U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 763 (1989) (stating privacy concept illustrated by FOIA exemption not limited or "cramped" notion).

against public intrusions.[51] Ultimately, the Court did not require disclosure of the photographs, concluding that the privacy interests of the deceased's family members outweighed the public's interest in disclosure.[52] Additionally, the Court suggested the case would require an entirely different analysis if the family argued for the deceased's privacy interests instead of their own.[53]

B. The Digital Era and Privacy

1. Federal Versus State Regulation of Digital Data

a. SCA and ECPA

In 1986, Congress enacted the SCA as part of the ECPA.[54] The SCA is a federal law governing the use and distribution of stored wired and electronic communications and transactions possessed by Internet service providers.[55] In general, the SCA prohibits unauthorized access in order to safeguard a user's privacy interests.[56] Moreover, the law forbids consumer electronic-communications companies from disclosing user content without an explicit exception, such as owner consent or government order.[57] Despite its

51. *See Favish*, 541 U.S. at 165-67 (interpreting language of FOIA exemption to determine Congress's intent); *see also* Christine M. Emery, Note, *Relational Privacy—A Right To Grieve in the Information Age: Halting the Digital Dissemination of Death-Scene Images*, 42 RUTGERS L.J. 765, 791-92 (2011) (arguing *Favish* Court affirmatively concluded deceased family members retain privacy rights against public intrusions).

52. *See Favish*, 541 U.S. at 171 (concluding deceased family's privacy interest outweighs public interest in disclosure). The Court stated that the requester was unable to demonstrate that disclosure of the photographs would likely advance public interest. *See id.* at 162. The Court additionally argued that because disclosure might infringe upon privacy interests, the requester must produce evidence showing a reasonable person might believe the government acted improperly in the investigation. *See id.* at 175.

53. *See id.* at 166 (indicating family invoked FOIA exemption on its behalf, not on behalf of deceased). The Court insinuated that the FOIA exemption does not protect the deceased's privacy interests, but rather protects the privacy interests of the deceased's family members:

> The family does not invoke Exemption 7(C) on behalf of [the decedent] in . . . fear that the pictures may reveal private information about [him] to the detriment of his own posthumous reputation or some other interest personal to him. If that were the case, a different set of considerations would control. [The deceased's] relatives instead invoke their own right and interest to personal privacy. They seek to be shielded by the exemption to secure their own refuge from a sensation-seeking culture for their own peace of mind and tranquility, not for the sake of the deceased.

Id.

54. *See* The SCA, 18 U.S.C. §§ 2701-2712 (2012) (addressing disclosure of third-party-held digital communications and transactional records).

55. *See id.* § 2702 (regulating Internet providers' disclosure of electronically stored communications and transactions); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide To Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) (describing third-party, Internet service provider as entity holding and processing user's information on user's behalf).

56. *See* Kendal Dobra, *An Executor's Duty Toward Digital Assets*, PRAC. LAW., Oct. 2013, at 21, 22 (explaining SCA's purpose to protect privacy interests in user's stored communications).

57. *See* The SCA, 18 U.S.C. § 2702 (2012) (prohibiting disclosure of user content unless owner consents

importance, the SCA nonetheless remains misunderstood, as courts, legislators, and scholars struggle with its meaning.[58] Furthermore, in the case of a deceased account holder, the SCA, or any other existing federal law, neither explicitly permits nor denies a fiduciary access to the deceased's electronic and stored communications.[59]

In the absence of federal regulation, state courts began issuing court orders demanding disclosure.[60] For instance, in 2005, a Michigan judge ordered Yahoo! to grant the family of a U.S. Marine killed in Iraq access to his email account.[61] Instead, Yahoo! provided copies of the email messages on a CD-ROM.[62] Nevertheless, finally in 2012, *In re Request for Order Requiring Facebook, Inc. to Produce Documents & Things*[63] addressed the complicated relationship between a service provider's compliance with the SCA and an executor's access to a deceased's digital assets.[64] There, the family of a decedent who died from apparent suicide sought access to her Facebook account to better understand the decedent's state of mind leading up to her death.[65] Relying on the SCA's privacy protections, the court held that a civil

or government issues order); *see also* William Bissett & David Kauffman, *Surf the Evolving Web of Laws Affecting Digital Assets*, 41 EST. PLAN. 32, 34 (2014) (discussing disclosure requirements in relation to content status). The SCA allows some service providers to disclose "non-content" electronic communications information to any person, except the government, without the user's consent. Bissett & Kauffman, *supra*, at 34. The SCA, however, states the service provider may divulge the "content" to a nongovernmental entity only if the account holder consents. *Id.*; *see also* Kerr, *supra* note 55, at 1223 (describing Section 2702(b) as providing eight exceptions for disclosure of content information).

58. *See* Kerr, *supra* note 55, at 1208 (describing SCA as "dense and confusing").

59. *See* Bissett & Kauffman, *supra* note 57, at 34-35 (arguing no federal regulation exists granting fiduciary access to decedent's digital content). Even if an individual possesses estate documents granting consent to a fiduciary to access the individual's electronic and stored communications, neither the SCA, nor any other existing federal law, recognizes the possibility for such a vested right. *See id.*

60. *See* Conner, *supra* note 5, at 301 (stating Michigan court ordered family access to deceased son's email account); *see also* Katy Steinmetz, *Your Digital Legacy: States Grapple with Protecting Our Data After We Die*, TIME (Nov. 29, 2012), http://techland.time.com/2012/11/29/digital-legacy-law/ [http://perma.cc/YYX9-SWXT] (arguing many states have no clear answer to solving digital assets question). In 2010, a Wisconsin judge ordered Google and Facebook to provide parents access to their son's accounts after his apparent suicide. *See* Steinmetz, *supra*. Although Google subsequently provided the parents access, Facebook only agreed to grant access on the condition that the parents sign a contract promising to never disclose the contents to anyone outside the immediate family. *See id.*

61. *See* Conner, *supra* note 5, at 301 (discussing Michigan court's decision to order family access to son's email account).

62. *See* Stefanie Olsen, *Yahoo Releases E-mail of Deceased Marine*, CNET (Apr. 21, 2005), http://news.cnet.com/Yahoo-releases-e-mail-of-deceased-Marine/2100-1038_3-5680025.html [http://perma.cc/MAB8-Z6ZL] (stating Yahoo! delivered CD-ROM of documents because of user privacy policy).

63. 923 F. Supp. 2d 1204 (N.D. Cal. 2012).

64. *See id.* at 1206 (granting Facebook's motion to quash subpoena on grounds subpoena violated SCA); *see also* Dobra, *supra* note 56, at 26 (describing *In re Facebook* holding as "merely one federal district court's interpretation of the SCA").

65. *See In re Facebook, Inc.*, 923 F. Supp. 2d at 1205 (discussing family's argument for gaining access to decedent's Facebook account). The decedent's family members disputed that she committed suicide and argued that her Facebook account contained critical evidence proving her state of mind right before her death. *See id.*

subpoena could not compel Facebook, or other service providers, to produce the decedent's records.[66] While the court stated Facebook could, on its own, determine whether the decedent's family has authorized access on the decedent's behalf, it ultimately declined jurisdiction over the issue.[67] Over the past decade, social-networking websites, like Facebook, began creating "deceased-user policies" to allow the family to determine what happens to the deceased user's account.[68] In the absence of clear legislation, however, online service providers continue to defer to preserving the user's privacy protection after death.[69]

b. Delaware's Fiduciary Access to Digital Assets and Digital Accounts Act

In August 2014, Delaware Governor Jack Markell signed the Fiduciary Access to Digital Assets and Digital Accounts Act into law, making the state the first to adopt a bill allowing fiduciary trustees access to, and control of, the online account and digital content of a deceased or incapacitated person.[70] Generally, access to a decedent's online account officially dies with the person.[71] Moreover, terms of service agreements between account users and

66. *See id.* at 1206 (holding compelling providers to produce decedent's records with civil subpoenas contradicts SCA's intentions); *see also* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y 2008) (holding SCA lacks exception for disclosure of electronic communications pursuant to civil subpoena); *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 610-11 (E.D. Va. 2008) (arguing statutory language of SCA does not exempt electronic communications pursuant to civil discovery subpoena).

67. *See In re Facebook, Inc.*, 923 F. Supp. 2d at 1206 (declining jurisdiction over whether Facebook could authorize access to decedent's family). The court stated that it lacked "jurisdiction to address whether the [decedent's family] may offer consent on [the decedent's] behalf so that Facebook may disclose the records voluntarily" and that "any such ruling would amount to nothing less than an impermissible advisory opinion." *Id.*; *see also* Dobra, *supra* note 56, at 25-26 (indicating court's holding did not prevent Facebook from voluntarily disclosing decedent's records).

68. Conner, *supra* note 5, at 309 (explaining deceased-user policies beginning to replace social-networking policies where control belongs to provider). Facebook's current policy allows the deceased user's family to choose to have the deceased's profile deleted from Facebook or memorialized. *See id.* Memorializing a profile, however, prevents anyone from logging into it at a future time. *See id.*

69. *See* Wilkens, *supra* note 6, at 1053 (noting online service providers' commitment to protecting users' privacy interests after death).

70. *See* DEL. CODE ANN. tit. 12, §§ 5001-5007 (West 2015) (regulating fiduciary access to decedent's digital accounts); *see also* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) (noting states may act as experimental laboratories when enacting new regulations); Caitlin Dewey, *What Happens to Your Online Life After You Die? Delaware Has Some Suggestions*, WASH. POST (Aug. 20, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/08/20/what-happens-to-your-online-life-after-you-die-delaware-has-some-suggestions/ [http://perma.cc/7PQT-KYF6] (describing Delaware legislation as "sweeping," while majority of states have no digital asset guidelines); Kate Tummarello, *Digital Access After Death Determined by Varying Federal, State Laws*, WARREN'S WASH. INTERNET DAILY, Jan. 31, 2013, at 1 (describing role of Uniform Law Commission in drafting digital asset legislation as model for states); Mordock, *supra* note 2 (noting several states' adoption of similar, but narrower, legislation, addressing only portion of digital communications).

71. *See* Cyrus Farivar, *Delaware Becomes First State To Give Executors Broad Digital Assets Access*, ARS TECHNICA (Aug. 18, 2014), http://arstechnica.com/tech-policy/2014/08/delaware-becomes-first-state-to-give-heirs-broad-digital-assets-access/ [http://perma.cc/R55A-H6NB] (stating access to deceased person's

digital providers, like Facebook, forbid access through password sharing between trusted individuals.[72] Under Delaware's newly enacted law, however, heirs and executors hold the same authority to take legal control of a decedent's digital assets, such as a digital account or device, as they would over a decedent's physical assets or documents.[73] Two major concerns emerged as a result of Delaware's broad legislation—first, whether the Delaware law conflicts with existing federal law, and second, whether it violates privacy rights because it assumes the decedent consents to access.[74] Nonetheless, it seems inevitable that Internet service providers in strong opposition to the Delaware law will likely challenge it, though some admit case law might help resolve the uncertainty.[75]

2. The Right To Be Forgotten Under European Law

In January 2012, the European Commissioner for Justice, Fundamental Rights, and Citizenship announced a proposal to create a new, extensive

digital account officially dies with person).

72. *See id.* (noting Facebook's terms of service agreement forbids password sharing with anyone, including spouse). According to Facebook's terms of service, the account holder shall "not share [his or her] password . . . let anyone else access [his or her] account, or do anything else that might jeopardize the security of [his or her] account." *Id.* Additionally, Facebook forbids an account holder from transferring his or her account to anyone without first obtaining Facebook's written permission. *See id.*; *see also Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/legal/terms (last updated Jan. 30, 2015) [http://perma.cc/8AVA-HU8P] (listing user's commitments to provider regarding registering and maintaining account security).

73. *See* DEL. CODE ANN. tit. 12, § 5005(a) (West 2015) (declaring fiduciary has same access as account holder). The Act states, "A fiduciary with authority over [account holder's] digital assets or digital accounts . . . shall have the same access as the account holder, and is deemed to: [h]ave the lawful consent of the account holder; and [b]e an authorized . . . user under all applicable state and federal law[s] . . . and any end user license agreement." *Id.* The new law may apply regardless of whether the parties live in Delaware; it may apply if Delaware governs the fiduciary relationship, such as if the person created his will under Delaware law, or if Delaware law grants someone power of attorney. *See* Miners, *supra* note 3 (arguing Delaware's new law has unlimited reach); *see also* Farivar, *supra* note 71 (explaining Delaware law grants heirs' and executors' broad, fiduciary access to deceased person's digital assets). Digital assets may constitute "online accounts and memberships, such as e-mail accounts, profiles on social-networking sites, online digital photo accounts, online banking and credit card accounts, websites or domain names owned by a person, and online subscription accounts." Conner, *supra* note 5, at 303; *see also* Dobra, *supra* note 56, at 22 (explaining difficulty of implementing universal definition of digital assets due to their constant evolution).

74. *See* The SCA, 18 U.S.C. §§ 2701-2712 (2012); *see also* Miners, *supra* note 3 (clarifying Internet industry's broad opposition to Delaware's new law). Specifically, Yahoo! and Facebook's criticism of Delaware's new law is due to the legislators' presumption that the deceased person would want his or her digital communications distributed. *See* Miners, *supra* note 3. The new legislation conflicts with the ECPA, which prohibits companies from disclosing user content without obtaining user consent. *See id.*; *see also* Mordock, *supra* note 2. "[A] court opinion will likely be necessary to resolve whether the legislation conflicts" with the ECPA, which prohibits "consumer electronic companies from disclosing content without the owner's consent or government order." Mordock, *supra* note 2.

75. *See* Mordock, *supra* note 2 (describing attorneys' prediction regarding legal challenge of Delaware's newly enacted law); *see also* Conner, *supra* note 5, at 314 (describing existing uncertainty as direct product of "new and unchartered territory" of Internet).

privacy right, otherwise known as "the right to be forgotten."[76] The right will allow individuals to remove information previously shared publicly while further prohibiting third party access to the information.[77] Account users will not only have the right to demand service providers to delete their data from public display, but also to ensure its deletion from the provider's archives.[78] Failure to comply may trigger liability for up to two percent of the provider's global income.[79] Through their proposal, European regulators sought to address the difficulty individuals face in escaping their past in the digital age, "now that the Internet records everything and forgets nothing."[80] Opponents argue, however, that Europeans tend to assert abstract privacy rights in theory without ever enforcing these rights in a practical sense.[81] Nonetheless, the right to be forgotten may serve better in practice as a postmortem right; although, U.S. critics argue its principles greatly conflict with American values—namely the right to free speech.[82]

76. *See* European Commission Press Release, Commission Proposes a Comprehensive Reform of Data Protection Rules To Increase Users' Control of Their Data and To Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm [https://perma.cc/7M95-4JK3] (proposing "right to be forgotten"); *see also Factsheet on the "Right To Be Forgotten" Ruling*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (last visited Mar. 10, 2015) [http://perma.cc/J494-FXVF] (explaining "right to be forgotten" proposal).

77. *Factsheet on the "Right To Be Forgotten" Ruling*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (last visited Mar. 10, 2015) [http://perma.cc/J494-FXVF] (stating individuals who remove their publicly shared information may require third parties to remove it). The proposal provides that when an individual demands the deletion of his or her personal data, the Internet service provider must timely obey. *See id.*

78. *See* Jeffrey Rosen, *The Right To Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 90 (2012) (explaining account users' rights against service providers under "right to be forgotten").

79. *See id.* at 88 (stating Internet providers must ensure removal of individual's personal data or face criminal sanctions). The "right to be forgotten" creates a legally enforceable right to demand deletion of any photos or personal data the individual posted himself or herself, even if the data went viral. *See id.* at 89.

80. *Id.* (discussing European regulators' concern of Internet data's permanent nature).

81. *See id.* at 92 (noting Europe often asserts abstract rights it fails to enforce); *see also* MADOFF, *supra* note 10, at 7 (discussing European regulators' perspective on postmortem privacy rights). European countries tend to be more concerned with the dignity of the dead, as some countries have governmental entities that specifically deal with protecting a person's privacy and reputational interests after death. *See* MADOFF, *supra* note 10, at 7.

82. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 864 (1997) (extending First Amendment protection to Internet speech); *see also* Ashcroft v. Am. Civil Liberties Union, 535 U.S. 564, 584-85 (2002) (affirming First Amendment protection to Internet speech as held in *Reno*); Steven C. Bennett, *The "Right To Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 168-69 (2012) (contrasting European Union's treatment of privacy rights with United States treatment of privacy rights). The European Union traditionally adheres to highly protected privacy rights, while the United States traditionally prioritizes freedom of expression over privacy. *See* Bennett, *supra*, at 168-69; *see also* Rosen, *supra* note 78, at 88 (arguing "right to be forgotten" as biggest threat to free Internet speech in coming decade). Not only can an individual assert the "right to be forgotten" against content publishers, such as Facebook, but also against search engines, like Google. *See* Rosen, *supra* note 78, at 91 (describing right to be forgotten as having "serious chilling effect"); *see also* Peter S. Vogel, *Free Speech vs. Internet Privacy and the 'Right To Be Forgotten,'* E-COMMERCE TIMES (June 10, 2014), http://www.ecommercetimes.com/story/80567.html [http://perma.cc/N3ZW-MH8M] (stating Google argues right creates "collision between [] right to be forgotten and [] right to know").

C. Descendible Postmortem Rights

1. Right of Publicity and Copyright Law

Although American law provides no privacy protections after death, the law has nonetheless evolved, granting the deceased other protections, including copyright protection and the right of publicity.[83] In general, the right of publicity affords an individual the right to control the commercial value of his or her name, image, and likeness.[84] Originally, the right of publicity limited protections to the individual's lifetime; however, over time, states enacted laws to extend its protections beyond death.[85] This change occurred because courts began to perceive the right of publicity as a property interest, rather than a personal interest.[86] Therefore, states provide protection to the decedent's heirs, who subsequently own the interests, because those interests possess economic value.[87]

The federal government established copyright law as another descendible postmortem right to provide the individual a short-term monopoly over his or her creative works.[88] The individual's work then becomes a part of the public domain after a specified period.[89] Over time, copyrights have become more valuable assets, and thus, American copyright protection today lasts up to

83. *See* MADOFF, *supra* note 10, at 7 (explaining evolution of law as copyright and right of publicity protections extend to deceased persons). Defamation and invasion of privacy claims may protect a person's reputational interests; however, such claims only protect a living person, and thereby extinguish upon the person's death. *See id.* at 6.

84. *See id*. at 10 (defining right of publicity). The right of publicity emerged as an element of the right to privacy. *See id*. at 132.

85. *See id.* at 10 (explaining right of publicity's evolution from originally protecting living persons to protecting deceased persons). Although the duration of protection varies between jurisdictions, most states grant protection until fifty years after death. *See id*.

86. *See* Haelan Labs., Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953) (holding right of publicity more akin to property interest than purely personal interest). The court held that the right of publicity was assignable, like a property interest. *See id.*; *see also* MADOFF, *supra* note 10, at 10 (explaining right of publicity's protection treated as property interest). Although the *Haelan* holding was insignificant at the time, the shift of the right of publicity from a purely personal interest to a property interest "transformed the legal landscape and paved the way for a new billion-dollar industry." MADOFF, *supra* note 10, at 134.

87. *See* MADOFF, *supra* note 10, at 10 (arguing extended protection created because right of publicity deemed economically valuable). The principal difference between the right of publicity and the right of privacy is arguably an economic one:

> The Right of Publicity is similar to the appropriation form of invasion of privacy. The principal difference is that the right of publicity seeks to ensure that a person is compensated for the commercial value of his name or likeness, while the right of privacy seeks to remedy any hurt feelings or embarrassment that a person may suffer from such publicity.

Mark Litwak, *The Right of Publicity*, ENT. L. RESOURCES BLOG (Dec. 2, 2011), http://www.marklitwak.com/blog/the-right-of-publicity [http://perma.cc/3ARN-EXUV].

88. *See* MADOFF, *supra* note 10, at 9, 141-42 (defining copyright law generally).

89. *See id.* at 9 (explaining copyright expiration).

seventy years after the creator's death.[90] Similar to the right of publicity, copyright protection does not die with the creator, arguably because it is also considered a property interest.[91] For example, for the last fifty years, All Hallows College kept 130 handwritten letters between an Irish priest and former first lady, Jackie Kennedy, hidden in a safe in Dublin, where the priest and Kennedy first met.[92] In June 2014, the college scheduled the letters for auction, with an estimated value of approximately 3.5 million dollars.[93] The collection of letters is essentially an autobiography, as it provides insight into Kennedy's private, personal thoughts following her husband's assassination.[94] When Jackie Kennedy died, she granted her writings and copyright interests to her children; however, her daughter Caroline Kennedy acquired complete control following her brother's death in a tragic plane crash.[95]

Shortly after the college announced the auction sale, the letters were pulled due to copyright and ownership concerns.[96] Under copyright law, the physical letter belongs to the recipient; however, that letter's copyright resides with the author.[97] Although the college claimed ownership of the letters, because Jackie Kennedy authored the letters, her copyright transferred to her heirs—in this

90. *See id.* at 141 (indicating copyright protection extended to last for seventy years after creator's death); *see also* Conner, *supra* note 5, at 306 (stating copyright protection lasts during person's lifetime and seventy years after death).

91. *See* MADOFF, *supra* note 10, at 141 (stating copyright expansion increased economic value of copyrights). The expansion of copyright resulted in some disadvantages; for instance, it included limited public access to protected creations. *See id.* The doctrines of the right to publicity and copyright both provide protections that "are strictly limited to economic, as opposed to reputational, interests." *Id.* at 131.

92. *See* Ed Carty, *Jackie Kennedy's Letters Are Pulled from Auction*, BELFAST TELEGRAPH (May 22, 2014), http://www.belfasttelegraph.co.uk/news/world-news/jackie-kennedys-letters-are-pulled-from-auction-30294436.html [http://perma.cc/AD3N-APCA] (discussing secret letters between Jackie Kennedy and Irish priest). The letters Jackie Kennedy wrote "strike a remarkable confessional tone" and "document the battles [Kennedy] had with her faith following her husband's assassination." *Id.*

93. *See id.* (estimating auction sale value of Kennedy letters at 2.4 million pounds); *see also* Matt Viser, *Jackie Kennedy Letters to Priest Pulled from Auction*, BOS. GLOBE (May 21, 2014), http://www.bostonglobe.com/news/nation/2014/05/21/trove-letters-jackie-kennedy-wrote-irish-priest-pulled-from-auction/Mii093KtvApnjJcHsFD4mN/story.html (estimating auction sale value of Kennedy letters could reach four million dollars).

94. *See* Carty, *supra* note 92 (stating collection of letters reveal Jackie's "private and innermost thoughts"); *see also* Viser, *supra* note 93 (describing letters as "deeply personal"); Matt Viser, *Kennedy Letters Fiercely Protected for Decades*, BOS. GLOBE (June 10, 2014), http://www.bostonglobe.com/news/nation/2014/06/09/with-kennedy-family-copyright-claims-letters-from-jackie-kennedy-hold-uncertain-future/UqIpwZkgptcJvBov9e4JbI/story.html (describing letters as revealing Jackie's most private thoughts on marriage, motherhood, and death). In the letters to Father Joseph Leonard, the Irish priest, Kennedy doubted her husband's faithfulness, mourned her son's death, and questioned her faith following her husband's assassination. *See* Viser, *supra* note 93.

95. *See* Viser, *Kennedy Letters Fiercely Protected for Decades*, *supra* note 94 (stating Caroline Kennedy acquired mother's copyright interests once JFK Jr. died in plane crash); *see also* MADOFF, *supra* note 10, at 143 (explaining copyright protection meant to benefit not only original creator but also creator's heirs).

96. *See* Viser, *Kennedy Letters Fiercely Protected for Decades*, *supra* note 94 (indicating reasons for pulling letters from auction).

97. *See id.* (discussing transfer of copyright interests from Jackie Kennedy to daughter, Caroline Kennedy, upon her death); *see also* MADOFF, *supra* note 10, at 9 (stating copyright law extends rights to deceased).

case Caroline Kennedy—upon her death.[98] Further, Jackie Kennedy wrote in her will, "I request, but do not direct, my children to respect my wish for privacy."[99] Caroline Kennedy, however, claimed ownership of the letters under a copyright theory, as opposed to a privacy theory.[100] Caroline Kennedy arguably preserved the privacy of her late mother in a strategic manner; rather than invoking a postmortem privacy right, which would be unfounded because no right exists, she asserted the postmortem right of copyright and established ownership to keep the letters secret.[101]

III. ANALYSIS

The uncertainty regarding whether or not heirs can legally access a decedent's online account could spark a debate in favor of a posthumous right to privacy.[102] Copyright and the right to publicity did not originally offer afterlife protections, but rather evolved into posthumous rights over time.[103] In light of this evolution, perhaps the digital era will call for a posthumous privacy right as federal, state, and private actors grapple with conflicting regulations.[104]

98. *See* Viser, *supra* note 93 (indicating college claims ownership of letters); *see also* MADOFF, *supra* note 10, at 131 (stating copyright protection continues even after person's death); Kirsten Rabe Smolensky, *Rights of the Dead*, 37 HOFSTRA L. REV. 763, 773 (2009) (explaining posthumous rights allow living person to enforce right while deceased benefits, like third-party beneficiaries); Viser, *Kennedy Letters Fiercely Protected for Decades*, *supra* note 94 (stating Jackie Kennedy's copyright interests transferred to daughter upon her death).

99. Viser, *Kennedy Letters Fiercely Protected for Decades*, *supra* note 94.

100. *See id.* (indicating Kennedy family asserted copyright ownership of letters). In 2003, a book published about the Kennedys contained a chapter based on interviews the author conducted with a Jesuit priest who counseled Jackie Kennedy after her husband's death. *See id.* The author also based the chapter on letters Kennedy wrote to the priest; those letters were available at Georgetown University. *See id.* Shortly after the author published the book, Caroline Kennedy claimed she owned the copyright to the letters, and Georgetown subsequently placed restrictions on the letters, preventing them from being viewed. *See id.*

101. *See* MADOFF, *supra* note 10, at 123-24 (indicating right of privacy does not continue after death). An individual can only utilize certain legal mechanisms, such as copyright law, to protect the reputation of a deceased person:

> The areas of law most directly concerned with reputation—defamation and privacy—strictly adhere to the position that a person has no interest in his or her reputation after death. Where reputational interests blend with or have been converted into property interests, however, the law has moved to granting greater rights to the dead, regardless of the costs imposed on the living.

Id. at 121.

102. *See Digital Access After Death Determined by Varying Federal, State Laws*, *supra* note 70 (noting legal uncertainty remains due to conflicting regulations affecting decedent's digital content). Under existing federal laws, such as the SCA, it remains uncertain whether access to a decedent's online data is allowable even with a court order. *See id.*; *see also* Mordock, *supra* note 2 (arguing uncertainty remains over accessibility of decedent's digital content).

103. *See* MADOFF, *supra* note 10, at 7-10 (explaining copyright and right of publicity evolution into posthumous rights).

104. *See Digital Access After Death Determined by Varying Federal, State Laws*, *supra* note 70 (arguing federal and state regulations of digital content conflict).

A. Posthumous Right to Privacy

1. Use of Descendible, Vested Rights To Preserve Privacy After Death

The evolution of copyright and the right of publicity into posthumous rights suggests that privacy protections after death are not a far-fetched theory.[105] Without afterlife privacy protections, the government forces families to rely on posthumous doctrines to protect a decedent's privacy.[106] For example, Caroline Kennedy invoked a copyright claim over private letters between her mother and an Irish priest to protect her late mother's privacy.[107]

An invasion of privacy claim does not apply once an individual dies because the law provides no protections for "reputational interests after death."[108] Unlike privacy, however, the right of publicity and copyright survive the creator for a specified time after his or her death.[109] This was not always true, as the doctrines in their traditional forms did not originally extend their protections after death.[110] Once courts considered copyright and the right of publicity as property interests, however, courts extended their protections—mainly for economic reasons.[111]

Nonetheless, families asserting copyright claims are perhaps motivated to protect privacy, not economic, interests.[112] For instance, an interest in protecting her mother's privacy, not her property, likely motivated Caroline Kennedy in asserting a copyright claim over her mother's private letters.[113]

105. *See* MADOFF, *supra* note 10, at 127 (questioning whether attacks on individual's reputation after death causes harm to decedent). Although posthumous harm is a complex issue, American law presumes the dead are unable to suffer from reputational assaults; therefore, the law does not protect reputational interests. *See id.* Rhode Island is the only state enforcing protections against defamation of the dead, which is a reputational interest like privacy, rather than a property interest. *See id.* at 123.

106. *See* Viser, *Kennedy Letters Fiercely Protected for Decades*, *supra* note 94 (explaining reliance on posthumous protections to preserve privacy rights).

107. *See id.* (indicating posthumous copyright protects Kennedy's privacy rights).

108. MADOFF, *supra* note 10, at 6. In *Favish*, the Court stated that the law cannot protect the infringement upon the decedent's privacy to the "detriment of his own posthumous reputation or some other interest personal to him." Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 166 (2004) (indicating Court's holding might differ if decedent's privacy protection invoked).

109. *See* MADOFF, *supra* note 10, at 6-7 (discussing copyright and right of publicity's evolution extending protection to deceased persons). Copyright law grants its holder an exclusive right to control his or her creative work for a specified time, after which the work becomes part of the public domain. *See id.* at 141. State law governs the posthumous duration of the right of publicity, which ranges from ten years to a century depending on the jurisdiction. *See id.* at 135.

110. *See id.* at 143 (noting first copyright law designed to last no longer than author's life). Like privacy rights, however, "the right of publicity traditionally died with the decedent, and estates were not allowed to bring suit to recover for the unauthorized use of the decedent's likeness." Smolensky, *supra* note 98, at 790.

111. *See* MADOFF, *supra* note 10, at 130-32 (arguing economic interests drove right of publicity and copyright's extended protections). The premise of the expansion in both these doctrines is protecting the dead; however, they award economic, instead of reputational, protections. *See id.* at 131.

112. *See supra* note 98 and accompanying text (explaining reliance on posthumous protections to protect decedent's privacy rights).

113. *See supra* note 98 and accompanying text (arguing Caroline Kennedy asserted copyright to protect

Therefore, if an individual asserts posthumous rights, such as copyright, to protect a decedent's privacy, it may be time to consider extending privacy protections after death.[114]

2. Theoretical and Practical Challenges to Privacy Protection After Death

The right of privacy is a fairly new principle in American history; therefore, there is potential for privacy law to evolve into a posthumous doctrine.[115] Although the Supreme Court has long held that the privacy right of the living is constitutionally protected, the same is not true for the dead.[116] The reason for the lack of privacy protections for the dead, however, is "both theoretical and practical."[117]

Theoretically, privacy law protects an individual from feeling embarrassed, and because a deceased person cannot feel embarrassed, he or she cannot suffer the harm that privacy law intends to protect.[118] Further, privacy law offers no practical mechanism for a decedent to assert an invasion of privacy interest posthumously.[119] For instance, the legal mechanism of probate, which appoints a representative for the decedent to distribute his or her estate, protects only a decedent's property interests.[120] Therefore, even if American law extended privacy protections to the dead, the law in its current form fails to employ a mechanism that represents the decedent's privacy interest after the individual has died.[121]

Likewise, utilizing the *Katz* expectation-of-privacy test to argue that a posthumous right to privacy should exist proves difficult.[122] The idea that a nonliving person exhibits an expectation of posthumous privacy and that such expectation is one society recognizes as reasonable is arguably a far-fetched

mother's privacy); *see also* Viser, *Kennedy Letters Fiercely Protected for Decades*, *supra* note 94 (stating in her will, Jackie Kennedy asked children to respect her privacy upon death).

114. *See* MADOFF, *supra* note 10, at 123 (describing right of privacy as "recent vintage"). The American law's recognition of the right of privacy did not originate from the English courts, but rather from scholars in the early twentieth century. *See id.*

115. *See id.* (claiming privacy right as fairly new concept in American law).

116. *See* Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 166 (2004) (distinguishing deceased's privacy interests from his surviving family's privacy interests). The Court held that the deceased's family members retained a protected privacy interest as survivors of the deceased. *See id.*; *see also* Schuyler v. Curtis, 42 N.E. 22, 25 (N.Y. 1895) (stating individual right of privacy dies with person). The right of privacy "is the right of the living and not that of the dead." *Schuyler*, 42 N.E. at 25.

117. MADOFF, *supra* note 10, at 125.

118. *See id.* (explaining American law's theoretical position for failing to provide posthumous privacy protection).

119. *See id.* (stating American law's practical reason for failing to protect dead's reputational interests).

120. *See id.* (arguing legal mechanism exists to protect decedent's property interests).

121. *See* MADOFF, *supra* note 10, at 125 (arguing no legal mechanism exists to allow assertion of decedents' privacy interests).

122. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (describing *Katz* expectation-of-privacy test).

assertion.[123] In fact, the *Jones* Court recognized the potential difficulty in applying the *Katz* test in the digital era to determine a person's expectation of privacy.[124]

The Supreme Court's dicta, however, suggests the digitization of content triggers a privacy concern.[125] Although the *Riley* Court's decision focused on the digital capabilities of cell phones, it acknowledged that digital content poses weightier privacy concerns than physical content due to its qualitative and quantitative nature.[126] Thus, if an individual challenges Delaware's digital asset law, a postmortem privacy right in the digital era might be debated under an equilibrium-adjustment theory.[127]

B. American Values of Privacy

Societal values, rather than theory or practicality, may signify another reason why American law does not extend privacy protections to the dead.[128] For instance, the United States "has traditionally emphasized freedom of expression over privacy, as a fundamental value," whereas most European countries "adhere[] to a high degree of government involvement" to protect this fundamental right.[129] Not only do European countries value privacy more than the United States, but they also place a higher value on the dignity of the dead.[130] For instance, certain governmental entities in Europe are specifically responsible for protecting a person's privacy and reputational interests after death, whereas American law fails to do the same.[131] The law reflects what and

123. *See id.* (explaining *Katz* test two-step analysis). American law's refusal to extend protection to the deceased's reputation "is often couched in terms of logic: after death there is no reputation to be harmed nor for the law to protect." MADOFF, *supra* note 10, at 127.

124. *See* United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) (predicting difficulty in determining individual's privacy expectations under *Katz* test in technological era).

125. *See* Riley v. California, 134 S. Ct. 2473, 2489-90 (2014) (highlighting cell phones' storage capacity as relevant toward inquiry into level of privacy concern). Specifically, the Court in *Riley* found that because modern devices, such as cell phones, possess immense storage capacities, they also trigger heightened privacy-related concerns. *See id.*

126. *See Riley*, 134 S. Ct. at 2489 (noting quantitative and qualitative nature of cell phones). "Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read." *Id.*

127. *See* DEL. CODE ANN. tit. 12, § 5004 (West 2015) (authorizing fiduciary access over digital assets); *see also* Kerr, *supra* note 45, at 480 (identifying equilibrium-adjustment theory as judicial response to privacy protections in technological age); Kerr, *supra* note 44 (describing *Riley* as "tip of [] iceberg" with how digital era changes application of Fourth Amendment); Mordock, *supra* note 2 (indicating courts will have final say on constitutionality of Delaware law).

128. *See* MADOFF, *supra* note 10, at 153 (arguing law reflects societal values). "[P]articular trade-offs that the law makes reflect what the society most values." *Id.* Although not explicitly stated, U.S. law "speaks volumes" about what society values most—whether the living or the dead. *Id.*

129. Bennett, *supra* note 82, at 168-69; *see also* Rosen, *supra* note 78, at 92 (arguing Europe has reputation of declaring abstract privacy rights although failing to practically implement them).

130. *See* MADOFF, *supra* note 10, at 7 (stating Europeans value dignity of dead, unlike Americans).

131. *See id.* (arguing different approach to rights of dead in United States and Europe).

who society values most; therefore, perhaps a change in American values must first occur for a posthumous privacy right to emerge.[132]

C. Conflicting Regulations Cause Uncertainty

Conflicting federal, state, and private regulations currently govern the state of an individual's digital account after death.[133] The disorderly scenario existing between regulators has caused legal uncertainty regarding a decedent's digital privacy.[134] On the one hand, Delaware state legislators grant fiduciary trustees access to, and control of, a decedent's online account and digital content.[135] On the other hand, service providers refuse to allow access, arguing that doing so violates their contractual obligation to protect user privacy.[136] Grieving families then seek court orders demanding providers to allow access to their loved ones' digital accounts.[137] Meanwhile, federal regulations, such as the SCA, forbid providers from disclosing user content.[138]

Additionally, the broad statutory language in Delaware's law further

132. *See id.* at 153 (discussing societal value effects on law).

133. *See* Bissett & Kauffman, *supra* note 57, at 33-34 (discussing Supremacy Clause's effect on state law conflicting with federal law); *see also* Wilkens, *supra* note 6, at 1053 (arguing "privacy laws leave questions of access after death largely unanswered"); Dewey, *supra* note 70 (predicting Delaware law could foreshadow national changes); Tummarello, *supra* note 70 (arguing conflict between federal, state, and private regulations governing posthumous online accounts); Mordock, *supra* note 2 (explaining concern over whether Delaware law and federal law conflict).

134. *See* Tummarello, *supra* note 70 (indicating varying laws result in legal uncertainty). Under established federal laws, such as the SCA, it is unclear whether an individual can access a decedent's online data, even with a court order. *See id.*; *see also* Mordock, *supra* note 2 (stating obtaining content of online communications remains uncertain).

135. *See* DEL. CODE ANN. tit. 12, § 5004 (West 2015) (granting rights to fiduciaries over digital assets); *see also* Dewey, *supra* note 70 (announcing passage of Delaware's digital asset law); Farivar, *supra* note 71 (stating Delaware law ensures family has access to decedent's digital assets); Gershman, *supra* note 8 (outlining additional control Delaware law grants to fiduciaries over decedent's online information).

136. *See* Farivar, *supra* note 71 (explaining Delaware law's unpopularity among technology companies). Not only are Internet service providers, such as Google, Yahoo!, and Facebook, concerned with the law's intrusion of privacy upon the user, but providers are also concerned with the privacy of third parties who communicated with the deceased online. *See id.*; *see also* Dewey, *supra* note 70 (admitting technology industry unhappy with legislation similar to Delaware's); Mordock, *supra* note 2 (noting technology companies' intent to challenge Delaware law). "Users expect [companies] to defend their privacy with a broad sword, so the companies have fought to protect that privacy even after the users are gone." Steinmetz, *supra* note 60 (arguing business model of technology companies depends on users' trust). Digital asset laws like Delaware's would force companies to violate their user agreements, which prevent access to unauthorized individuals. *See* Tummarello, *supra* note 70. Moreover, users choose online providers based on the privacy protections they offer in their terms-of-service agreements. *See id.*; *see also* Miners, *supra* note 3 (stating Yahoo!'s opposition to Delaware law due to user privacy concerns). "Without clear legislative guidance, online service providers have erred on the side of protecting privacy, even after death." Wilkens, *supra* note 6, at 1053.

137. *See* Conner, *supra* note 5, at 301 (discussing Michigan court order granting family access to deceased son's email account); *see also* Steinmetz, *supra* note 60 (discussing Wisconsin court order providing parents access to son's online accounts).

138. *See* The SCA, 18 U.S.C. § 2702 (2012) (prohibiting companies from disclosing user content).

complicates the matter.[139] The Delaware law allows fiduciary trustees control of and access to a decedent's online account.[140] A fiduciary is authorized to control the rights in a decedent's online account "to the extent permitted under applicable state or federal law . . . or any end user license agreement."[141] With regard to access, however, a fiduciary has the same *access* as a decedent and is considered "an authorized agent or user under all applicable state and federal law and regulations and any end user license agreement."[142] In other words, Delaware's legislation does not limit a fiduciary's *access* based on federal or private regulations, but it does limit a fiduciary's *control* of the rights in a decedent's online account.[143]

Delaware legislation presumes any and all regulation applicable to a user's online access classifies a fiduciary as an authorized user.[144] Even if a decedent grants access to a fiduciary, however, neither the SCA nor any other existing federal law recognizes a vested right.[145] Perhaps Delaware's broad presumption is the reason critics describe the legislation as a "novel approach" to posthumous, digital privacy concerns.[146] The Delaware law, however, may be considered ingenious despite the criticism, as states arguably should function as laboratories of democracy under a federal system that makes them capable of trying "novel social and economic experiments without risk to the rest of the country."[147]

IV. CONCLUSION

Given the discrepancy in federal, state, and private regulations, the debate over whether a posthumous privacy right exists is likely to continue. Meanwhile, practical and theoretical factors challenge the possibility for afterlife privacy protections. Copyright and the right of publicity, however, have evolved into posthumous rights. Therefore, it is plausible privacy

139. *See* DEL. CODE ANN. tit. 12, § 5004(a) (West 2015) (stating fiduciary has control over "any and all rights in digital assets and digital accounts"); *see also* Farivar, *supra* note 71 (highlighting breadth of Delaware's digital asset laws compared to those of other states).

140. *See* DEL. CODE ANN. tit. 12, § 5004(a) (West 2015) (providing fiduciaries control over deceased's digital data).

141. *Id.*

142. *Id.* § 5005(a).

143. *See* Miners, *supra* note 3 (noting Delaware law permits "broad" access).

144. *See* Tummarello, *supra* note 70 (presuming state law authorizes fiduciaries, acting on behalf of deceased users, to give required consent). Although Congress may reform federal laws, such as the SCA, the Uniform Law Commission's drafting committee "tiptoes" around the outdated federal laws currently enacted. *Id.*

145. *See* Bissett & Kauffman, *supra* note 57, at 34-35 (noting no existing federal law recognizes fiduciary access to deceased users' digital accounts).

146. Gershman, *supra* note 8.

147. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting). "It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory." *Id.*

protections will change in a similar manner. This likelihood is especially true if a family, like the Kennedys, strategically asserts copyright to preserve a loved one's privacy after death. Today, there is no definite answer as to what happens to a person's online data after death. Perhaps states would be wise to pass sweeping digital asset legislation, much like Delaware has already enacted, in an attempt to influence this uncertain area of the law and best expedite a concrete solution.

Melissa Gaied