The "PEAC" of Digital Estate Legislation in the United States: Should States "Like" That?

"Millions of us live whole facets of our lives in the virtual world, facets that will be left behind, and potentially unavailable to executors and trustees. An increasing number of people, all of whom will die one day, maintain Facebook identities, online bank accounts, libraries of downloaded music, personal photo archives and email. Tying up digital loose ends can be harder than tidying up paper, and the prospect of millions of digital deaths has raised legal questions that remain largely unanswered."[1]

I. INTRODUCTION

In an increasingly digital society, individuals store information online and occupy a social media presence more than ever.[2] Whether through Facebook or other social networking platforms, email accounts, online banking, music providers, or other digital outlets, society occupies and possesses vast digital property.[3] Many types of digital property are replacing—or have already replaced—outdated types of tangible personal property.[4] Further, unlike our friends and family, whose lives must, unfortunately, come to a halt, digital property can exist into perpetuity.[5] Because laws addressing digital property

1. Amber Nimocks, *Don't Die Just Yet: Digital Death: Your Heirs May Find the Digital Assets You Left Behind Beyond Their Reach*, N.C. LAW. WKLY., Nov. 6, 2013, 2013 WLNR 28415152. Nimocks noted adaptation of the law is necessary notwithstanding the complexities surrounding the matter of "digital death." *Id.*

2. *See* Naomi Cahn, *Postmortem Life On-Line*, 25 PROB. & PROP. 36, 36-37 (2011) (explaining digital assets categorization and considering "client's on-line life" management); Maria Perrone, Comment, *What Happens When We Die: Estate Planning of Digital Assets*, 21 COMMLAW CONSPECTUS 185, 185-86 (2012) (considering various digital assets categories forming person's digital estate); Kristina Sherry, Comment, *What Happens to Our Facebook Accounts When We Die?: Probate Versus Policy and the Fate of Social-Media Assets Postmortem*, 40 PEPP. L. REV. 185, 186 (2012) (detailing increasing prevalence and importance of Internet and social media use throughout society).

3. *See* Greg Lastowka & Trisha Hall, *Living and Dying in a Virtual World: Estate Planning for Digital Assets*, 284 N.J. LAW. 29, 29 (2013) (using term "digital assets" to describe substantial portion of decedents' postmortem assets). Presently, more than one billion people possess Facebook profiles, and about the same number utilize Yahoo!, Gmail, or Hotmail email services. *See id.*

4. *See id.* (explaining uses of current digital property akin to functions of personal tangible property). For instance, "[a] decedent's digital photography archive on Flickr (or Instagram, Smugmug, or Picasa) might serve the same purpose as an old-fashioned shoe-box." *Id.* Alternatively, online financial service platforms often serve a purpose akin to traditional bank accounts. *See id.*

5. *See* Emily Stutts, *Will Your Digital Music and E-Book Libraries "Die Hard" With You?: Transferring Digital Music and E-Books Upon Death*, 16 SMU SCI. & TECH. L. REV. 371, 397 (2013) (highlighting potential for digital privacy agreements to extend into perpetuity).

implications upon death cannot keep pace with society's rapid technological revolution, digital estate law across the United States remains complicated and inconsistent.[6]

Presently, the majority of states prohibit family members and heirs from accessing information that a decedent stores online.[7] Further, privacy agreements between account holders and Internet Service Providers (ISPs) narrowly restrict access to digital accounts, creating obstacles for family members attempting to access such accounts following the death of a loved one.[8] In response, states have begun addressing the ambiguities regarding treatment of digital property by implementing legislation that governs digital assets.[9] Most notably, in 2014, Delaware became the first state to pass broad, comprehensive legislation regulating the access and use of digital assets upon death.[10]

Delaware's Fiduciary Access to Digital Assets and Digital Accounts Act (FADADAA) grants fiduciaries broad authority over the digital accounts or property of a decedent in the same way that fiduciaries inherit physical assets.[11] Based on suggested legislation from the Uniform Law Commission's Uniform Fiduciary Access to Digital Assets Act (UFADAA), citizens of Delaware are among the first to obtain inheritance rights as fiduciaries, which expand beyond the mere use or access to digital property.[12] Simultaneously, however, as states

6. *See* Siobhán Kinealy, *Night of the Living Data: Estates Law and the Phenomenon of Digital Life After Death*, 11 RUTGERS BUS. L. REV. 35, 36 (2014) (considering inconsistent and inadequate state laws despite increasing presence of digital assets); Ashley F. Watkins, Comment, *Digital Properties and Death: What Will Your Heirs Have Access to After You Die?*, 62 BUFF. L. REV. 193, 197-98 (2014) (detailing lack of legislation among majority of states leading to uncertain and inconsistent law); *see also* Tyler G. Tarney, Comment, *A Call for Legislation To Permit the Transfer of Digital Assets at Death*, 40 CAP. U. L. REV. 773, 775 (2012) (detailing uncertainty in law based on lack of state statutes or court decisions).

7. *See* Watkins, *supra* note 6, at 220-21 (citing seven state laws currently governing digital assets).

8. *See* Sherry, *supra* note 2, at 204-05 (explaining potential impact of user agreements specifying conditions for social media accounts postmortem).

9. *See id.* at 215-28 (detailing state legislation devising treatment of digital assets as probate property); *see also Acts: Fiduciary Access to Digital Assets, Revised (2015)*, UNIFORM L. COMMISSION, http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015) (last visited Mar. 31, 2016) [https://perma.cc/W3RB-ZL5D] (listing twenty-seven states considering passing—or already enacted—uniform digital asset legislation as of March 2016).

10. *See* Act of Aug. 12, 2014, ch. 416, 2014 Del. Laws 416 (codified at DEL. CODE ANN. tit. 12, § 5004 (West 2015)) (granting broad authority to fiduciaries over digital accounts or digital assets governed within Delaware); *see also* Michael Carney, *When You Die in Delaware, Your Digital Assets Become Part of Your Estate*, PANDO (Aug. 20, 2014), http://pando.com/2014/08/20/when-you-die-in-delaware-your-digital-assets-become-part-of-your-estate/ [http://perma.cc/HEU6-KPTU] (stating Delaware first state to sign bill on decedent's digital assets).

11. *See* DEL. CODE ANN. tit. 12, § 5004 (West 2015) (allowing fiduciary control beyond mere access of digital accounts and digital assets).

12. *See* Carney, *supra* note 10 (describing Delaware as first state to pass comprehensive legislation regarding postmortem digital assets); *see also* Susan Linda Ross, *Social Media Accounts After Death—Delaware's New Law*, MONDAQ, Sept. 19, 2014, 2014 WLNR 26055168 (noting Delaware's law modeled after Uniform Law Commission's suggested digital asset legislation).

begin to progress in the regulation of digital assets, federal law requirements create an additional layer of complication regarding the treatment of digital estates.[13] Legal commentators frequently cite federal legislation governing digital assets, including the Stored Communications Act (SCA) and Computer Fraud and Abuse Act (CFAA), as obstacles preventing ISPs from divulging digital account content to individuals other than the deceased account holder.[14] Thus, the coexistence of federal and state law governing access to digital property continues to muddy the water in this area of law, raising potential preemption and conflict of law issues.[15]

This Note explores the legal implications of recent digital assets legislation, suggested model legislation, and the future for digital estate planning generally.[16] First, this Note delineates the current state of federal law governing digital assets.[17] Additionally, this Note considers the consequences of Terms of Service (TOS) contracts in relation to the preservation of and access to digital account contents.[18] Next, this Note tracks the history and development of state legislation concerning postmortem digital assets.[19] Further, this Note surveys the development and implementation of suggested model legislation.[20]

This Note argues that federal and state law can coexist in this arena, as recent state law is complementary, not incompatible, with federal laws governing digital communications.[21] Further, this Note emphasizes the unique privacy concerns relevant to digital asset management, arguing sweeping state legislation that categorically divulges private account contents neglects the important privacy interests associated with such digital property.[22] Additionally, this Note highlights the importance of deferring to the decedent account holder's intent when determining whether fiduciary access or control over account content is appropriate after death.[23] This Note discusses areas of

13. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002) (detailing Stored Communications Act's legislative purpose while acknowledging congressional intent to protect private electronic communications); *see also* Allen D. Hankins, Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295, 297-311 (2012) (explaining protection afforded to communication under SCA and SCA's possible application).

14. *See* James D. Lamm et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. MIAMI L. REV. 385, 400, 403 (2014) (explaining risk of criminal prosecution when fiduciaries access decedent's digital assets).

15. *See id.* at 415 (explaining conflicts among state and federal digital assets laws raise federalism and preemption concerns).

16. *See infra* Part III.

17. *See infra* Part II.A.

18. *See infra* Part II.B.

19. *See infra* Part II.C.

20. *See infra* Parts II.D-G.

21. *See infra* Part III.A.

22. *See infra* Part III.B.

23. *See infra* Part III.C.

strength in current model legislation, namely the Privacy Expectation Afterlife and Choices Act (PEAC), which provides a useful example for states seeking to adopt comprehensive legislation recognizing the intimate and private nature of online property, even after death.[24] This Note concludes suggesting a court ruling is necessary to clarify the law concerning postmortem digital assets.[25]

II. HISTORY

A. Federal Legislation Governing Digital Assets

1. The SCA and CFAA

Currently, federal legislation governing digital assets consists of two federal laws: the SCA and CFAA.[26] In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), which included the SCA.[27] Recognizing the Fourth Amendment's failure to keep pace with the privacy implications of the Internet Age, Congress enacted the SCA in an attempt to fill a void in modern privacy protections for Internet communications.[28] Congress sought to prevent ISPs from exposing certain private communications to various entities and individuals.[29] Most notably, the SCA prohibits granting access or providing disclosure of electronic account content to individuals without the proper authorization.[30] More specifically, the SCA's prohibitions

24. *See infra* Part III.C.

25. *See infra* Part IV.

26. *See* CFAA, 18 U.S.C. § 1030 (2012) (criminalizing unauthorized or fraudulent computer access); SCA, 18 U.S.C. § 2701 (2012) (governing illegal retrieval of stored communications); *see also* MARY F. RADFORD, GEORGIA GUARDIANSHIP AND CONSERVATORSHIP § 5:14 (2014) (noting only two federal laws, CFAA and SCA, address accessing digital property).

27. *See* 18 U.S.C. § 2701(a)(1) (punishing deliberate retrieval of electronically stored communication in absence of authorization).

28. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 971 (C.D. Cal. 2010) (noting SCA passed to address rise in potential privacy concern resulting from creation of Internet). The court in *Crispin* recognized that all of the SCA's restrictions can apply to one service provider, recognizing that Facebook qualified as an electronic communication service (ECS) in some capacities and as a remote computing service (RCS) in others. *See id.* at 989-90; *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, 1209-13 (2004) (explaining legislative intent behind SCA). The SCA created privacy protections for online communications that the Fourth Amendment did not adequately consider. *See* Kerr, *supra*, at 1210. For example, the SCA restricted the government's authority to require disclosure of information in the possession of Internet providers. *See id.* at 1212. Further, the statute confines the power of ISPs, restricting the voluntary transfer of user information to government entities. *See id.* at 1213; *see also* 18 U.S.C. § 2702 (2012).

29. *See* Matt Borden, Note, *Covering Your Digital Assets: Why the Stored Communications Act Stands in the Way of Digital Inheritance*, 75 OHIO ST. L.J. 405, 414 (2014) (noting purpose and effect of Congress's SCA). Specifically, the relevant SCA provision that applies to ISPs acts as a potential prohibition on the voluntary disclosure of electronic communications. *See id.*

30. *See* 18 U.S.C. § 2702 (2012) (defining "voluntary disclosure of customer communications or records"). The SCA prohibits electronic communication service providers from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." *Id.*; *see also*

on the disclosure of electronic communications narrowly apply to remote computing services and electronic communication services.[31] Further, the SCA includes exceptions that account for situations where the disclosure of communications is appropriate, such as through the originator's legal consent or court order.[32] Another relevant federal provision, the CFAA, provides context—and simultaneous complication—for fiduciaries seeking to assert control over digital assets.[33] The CFAA governs fraudulent and other related criminal conduct related to computers, punishing willful access to obtain information from a computer without proper authorization.[34]

Courts reviewing the SCA have interpreted it to apply to web hosting and social networking websites.[35] In *Viacom International Inc. v. Youtube Inc.*,[36] a federal district court considered whether the plaintiff could compel the defendant to produce "private" videos, inquiring whether the ECPA barred disclosure.[37] The court held that the ECPA prohibited defendants from disclosing private videos while emphasizing that the user intentionally limited the public's access through only affording specific individuals access.[38] In

David Horton, *Indescendibility*, 102 CALIF. L. REV. 543, 569-70 (2014) (arguing SCA prevents descendibility of social networking accounts upon death); Borden, *supra* note 29, at 413 (describing SCA Section 2702's "voluntary disclosure provision" as most relevant to inheritance of digital assets). Further, the voluntary disclosure provision that regulates "public providers of electronic communication" most substantially affects social networking providers in the context of digital asset inheritance. *See* Borden, *supra* note 29, at 414.

31. *See* 18 U.S.C. § 2702(a) (2012) (explaining limited application of SCA prohibitions).

32. *See id*. § 2702(b) (listing consent of originator, addressee, or intended recipient as exception allowing disclosure of electronic communications). This SCA provision provides for circumstances where a provider is permitted to expose the contents of electronic communications. *See id.* One relevant exception allows for divulging communication contents where the provider receives the "lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." *Id.* § 2702(b)(3); *see also* Borden, *supra* note 29, at 417 (noting important exceptions in SCA). The consent exception allows ISPs to provide content or account information on the condition that the account holder expressly consents. *See* Borden, *supra* note 29, at 417. Additionally, the court order exception removes liability from ISPs when they disclose information pursuant to a court order, regardless of whether the decedent account holder consented. *See id.*

33. *See* 18 U.S.C. § 1030(a)(2) (2012) (providing criminal penalties for anyone who intentionally accesses computer, and information, sans authorization).

34. *See id.* (criminalizing intentional access to computer without, or exceeding, authorization). Specifically, the CFAA prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." *Id.* § 1030(a)(2)(c). The CFAA defines "protected computer[s]" as those "used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B). To satisfy this definition and CFAA application, courts construe the utilization of computers as inherently interstate based on the computer's nearly universal ability to access the Internet. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000). Further, although the CFAA does not elaborate upon the meaning of "authorization" or "authorized access," courts have broadly interpreted such terms to include any—even very limited—permission for access. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132-33 (9th Cir. 2009).

35. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980-81 (C.D. Cal. 2010) (deeming social networking sites qualified for application of SCA).

36. 253 F.R.D. 256 (S.D.N.Y. 2008).

37. *See id.* at 264-65 (applying ECPA to private YouTube videos).

38. *See id.* (rejecting plaintiff's argument concerning appropriateness of disclosure based on YouTube's

prohibiting disclosure of the private videos under the ECPA, the court reasoned that as an entity providing remote computing services to the public, YouTube is prohibited from "knowingly divulg[ing]" their subscribers' stored communication to any person or entity.[39]

Additionally, in *Bower v. Bower*,[40] a federal district court considered the SCA's application to the compelled disclosure of emails in response to civil discovery requests.[41] The court held that the SCA's prohibition on disclosure of contents to third parties barred the sought production at issue.[42] Importantly, the court emphasized the privacy interests at stake, which tipped the scale toward disallowing disclosure.[43]

2. SCA Application with Other Laws

The Supremacy Clause of the Constitution provides, "[T]he Laws of the United States . . . shall be the supreme Law of the Land."[44] Courts interpret this clause to require federal law to trump state law when the laws are in direct conflict.[45] Although acknowledging certain powers as within the state's legitimate police powers, the Court recognizes several types of preemption: express preemption, field preemption, conflict preemption, and complete preemption.[46] The Court acknowledges conflict preemption in situations where

privacy policy). The court explained that none of the clauses within the user's privacy policy with YouTube allow interpretation as permission to reveal private videos to the public. *See id.* at 265. The court further emphasized that the user designated the videos as private and chose only to share their content with specific individuals. *See id.*

39. *Id.* at 264.

40. 808 F. Supp. 2d 348 (D. Mass. 2011).

41. *See id.* at 350-51 (holding SCA prohibits social media providers from producing contents pursuant to civil discovery subpoenas). The court recognized that although the SCA permits the government to mandate disclosure in criminal investigations, civil litigants find no authority in the SCA to require disclosure of communications. *See id.* at 350. The court in *Viacom Int'l* also recognized that the ECPA applies equally to disclosures sought through civil discovery requests. *See* 253 F.R.D. at 264; *see also In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611-12 (E.D. Va. 2008) (recognizing exception to ECPA does not exist for civil discovery requests).

42. *See Bower*, 808 F. Supp. 2d at 349 (barring disclosure and rejecting argument defendant implicitly consented to document production).

43. *See id.* at 350 (emphasizing privacy concerns underlying SCA's general prohibition on disclosure of electronic communications to unauthorized users). Similarly, in *In re Subpoena Duces Tecum to AOL, LLC*, the court noted that the ECPA constructs "a zone of privacy," shielding unwarranted individuals or entities from inappropriately utilizing or divulging Internet users' intimate account content. *See* 550 F. Supp. 2d at 610.

44. U.S. CONST. art. VI, cl. 2.

45. *See* Mass. Ass'n of Health Maint. Orgs. v. Ruthardt, 194 F.3d 176, 178 (1st Cir. 1999) ("By virtue of this commandment, state law that conflicts with federal law is a nullity."); *see also* Maryland v. Louisiana, 451 U.S. 725, 746 (1981) (declaring, pursuant to Supremacy Clause, contrary state requirements lack effect).

46. *See* Barnett Bank of Marion Cty., N.A. v. Nelson, 517 U.S. 25, 31 (1996) (considering federal statute authorizing national banks to participate in conduct state law expressly forbids). The Court discussed the need to examine congressional intent in determining preemption issues. *See id.* Further, the Court recognized that explicit language indicating preemption is unnecessary; the Court can infer preemption through interpreting a federal statute's "structure or purpose." *Id.*; *see also* SPGGC, LLC v. Ayotte, 488 F.3d 525, 530-31 (1st Cir.

state law "irreconcilabl[y] conflict[s]" with federal law, positioning state law as an obstruction to Congress's achievement of legislative goals.[47]

In *Telecommunications Regulatory Board of Puerto Rico v. CTIA—The Wireless Ass'n*,[48] the First Circuit Court of Appeals considered a Puerto Rican law that authorized telephone companies to obtain information regarding prepaid cellphone holders.[49] The Puerto Rican law, the Registry Act, required telephone companies to provide the Puerto Rican government with various private details about their phone customers.[50] The court held the SCA preempted the application of Puerto Rico's law.[51] The First Circuit expressed concern that the Registry Act required what the SCA expressly prohibited, effectively preempting the Registry Act.[52]

B. Implications of Private Terms of Service Contracts

TOS contracts between decedent account holders and social media platforms create an additional layer of complication and confusion regarding the treatment of digital assets after death.[53] Specifically, many TOS contracts forbid fiduciary access and restrict transferring an account or the account's private contents after death.[54] Although social media providers almost universally err on the side of caution in the treatment of digital assets postmortem, because each service agreement's terms often vary, it fosters a lack of uniformity.[55] Some social media platforms provide that sharing your

2007) (discussing field preemption).

47. *Barnett Bank of Marion Cty.*, 517 U.S. at 31; *see also* California v. ARC Am. Corp., 490 U.S. 93, 100-01 (1989) (detailing situations where conflict preemption arises). The Court describes conflict preemption as "when compliance with both state and federal law is impossible, or when the state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objective of Congress.'" *ARC Am. Corp.*, 490 U.S. at 100-01 (citation omitted); *see also* Weaver's Cove Energy, LLC v. R.I. Coastal Res. Mgmt. Council, 589 F.3d 458, 472 (1st Cir. 2009) (affirming district court finding of preemption based on theory of conflict preemption).

48. 752 F.3d 60 (1st Cir. 2014).

49. *See id.* at 61 (finding SCA preempted application of Puerto Rican registration law, akin to state law).

50. *See id.* at 62 (discussing requirements of Puerto Rican law).

51. *See id.* at 68 (holding Puerto Rico Registry Act conflicts with SCA).

52. *See CTIA—The Wireless Ass'n*, 752 F.3d at 68 (finding SCA preempts Registry Act because of SCA's express prohibition on disclosure). The court discussed the history and purpose of the SCA, explaining its goal to modernize and refine federal privacy safeguards in response to escalating technological development and expansion. *See id.* at 64; *see also* S. REP. NO. 99-541, at 1 (1986). Nonetheless, the court recognized grounds in the statute's express language led to preemption, finding no need to look to legislative history to infer congressional intent. *See CTIA—The Wireless Ass'n*, 752 F.3d at 66. Without relying exclusively on legislative intent, to reject the appellant's arguments against preemption, the court noted the combined weight of unambiguous statutory language and legislative history conflicts with appellant's theory. *See id.* at 68.

53. *See* Watkins, *supra* note 6, at 216-18 (noting TOS can influence postmortem allocation of digital assets).

54. *See* Sherry, *supra* note 2, at 204 (noting social media providers' nontransferability and termination provisions may prevent passage of account contents); Watkins, *supra* note 6, at 217-18 (explaining many TOS agreements contain clauses prohibiting postmortem account transfer).

55. *See* Noam Kutler, *Protecting Your Online You: A New Approach To Handling Your Online Persona*

password for a digital account constitutes a TOS violation.[56] Other agreements require that an account holder agrees that access to an account is nontransferable, which empowers social media providers to terminate account contents upon the decedent account holder's death.[57]

C. Moving Toward Uniform State Legislation . . . Perhaps

In recent years, several states considered the governance of postmortem digital assets, and various states enacted statutes governing the property of deceased individuals.[58] In 2005, Connecticut passed the Access to Decedent's Electronic Mail Accounts Act, becoming the first state to enact legislation in this area.[59] The Connecticut statute narrowly applies to email accounts, providing executors or administrators with access to the contents of a deceased person's email account.[60] The Connecticut statute requires either the executor's written request for access, accompanied by both a copy of the death certificate and the executor's certificate of appointment or an order from the probate court with jurisdiction over the matter.[61] Although Connecticut's statute thoroughly addresses postmortem governance of a decedent's email accounts, the legislature confined the statute's coverage to only email-related property.[62] Connecticut's statute does not provide guidance for managing any other type of digital property and thus excludes regulation of social media

After Death, 26 BERKELEY TECH. L.J. 1641, 1644 (2011) (citing extensive differences between service agreements for creating confusion in handling postmortem digital assets).

56. *See, e.g.*, *Google Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms/ (last updated Apr. 14, 2014) [http://perma.cc/BF6U-MMAF] (providing safeguarding Google Account access requires restricting access to password); *Microsoft Services Agreement*, MICROSOFT (June 4, 2015), http://microsoft.com/en-us/servicesagreement/ [http://perma.cc/C5R2-3KZU] (noting responsibility to protect account information and maintain password confidentiality); *Yahoo Terms of Service*, YAHOO!, http://policies.yahoo.com/us/en/yahoo/terms/utos/index.html (last updated Mar. 16, 2012) [http://perma.cc/9TUR-ZXZ6] (detailing responsibility account holder maintain confidentiality of password).

57. *See Yahoo Terms of Service*, *supra* note 56 (providing for "No Right of Survivorship and Non-Transferability"). An individual creating a Yahoo! account acknowledges that the account is not transferable and upon death, forfeits rights in the account and its contents. *See id.* Further, after receiving a copy of the death certificate, the provider may permanently delete the account and its contents. *See id.*; *see also iCloud Terms and Conditions*, APPLE, https://www.apple.com/legal/internet-services/icloud/en/terms.html (last updated Sept. 16, 2015) [https://perma.cc/WQL2-TTKP]. Similarly, Apple account holders possess no right of survivorship, making all rights to an Apple ID or content stored terminate upon death. *See iCloud Terms and Conditions*, *supra*.

58. *See* Naomi Cahn, *Probate Law Meets the Digital Age*, 67 VAND. L. REV. 1697, 1721 (2014) (noting increasing consideration of digital assets legislation among states); Chelsea Ray, Note, '*Til Death Do Us Part: A Proposal for Handling Digital Assets After Death*, 47 REAL PROP. TR. & EST. L.J. 583, 601-04 (2013) (discussing current state legislation governing digital property after death).

59. *See* CONN. GEN. STAT. ANN. § 45a-334a (West 2015) (describing Connecticut state law governing postmortem access to decedent's email accounts).

60. *See id.* §§ 45a-334a(a)(1), (b) (limiting statute's application to "electronic mail service provider[s]").

61. *See id.* § 45a-334a(b) (stating document requirements before allowing access).

62. *See id.* § 45a-334a(a)(1) (defining statutory governance to merely include "intermediar[ies] [] sending or receiving electronic mail").

accounts, online banking accounts, and more.[63]

Similarly, in 2007, Rhode Island passed the Access to Decedents' Electronic Mail Accounts Act, which—in an almost identical way to the Connecticut statute—limits the law's application to the deceased account holder's email accounts.[64] The Rhode Island legislature similarly failed to account for many other important types of digital property, confining the law's scope to an executor's access to email accounts.[65]

Additionally, in 2007, Indiana enacted a slightly more expansive state statute governing a deceased's digital accounts.[66] The law provides a deceased person's personal representative with "access to or copies of any documents or information of the deceased person stored electronically."[67] Although Indiana's statute provides management beyond email accounts, the statute fails to define or clarify "documents or information."[68] Thus, the Indiana legislature left personal representatives or executors uncertain as to what type of digital accounts they may access in fulfilling their estate administration duties.[69]

Furthermore, Idaho and Oklahoma enacted similar legislation providing added guidance in the governance of postmortem digital property in 2011 and 2010, respectively.[70] Idaho's modified statute empowers the conservator, an individual analogous to a personal representative, with authority to "[t]ake control of, conduct, continue or terminate any accounts of the protected person on any social networking website, any microblogging or short message service website or any e-mail service website."[71] Similarly, in 2010, Oklahoma enacted a near mirror image law to Idaho's; the law's one distinction was establishing authority in the executor or estate administrator rather than the conservator.[72] Notably, though, this law received criticism for failing to

63. *See* CONN. GEN. STAT. ANN. § 45a-334a(b) (West 2015) (failing to include other Internet accounts in law's narrow application to email providers).

64. *See* 33 R.I. GEN. LAWS ANN. § 33-27-3 (West 2014) (detailing Rhode Island's legislation proscribing executor access to electronic mail of decedent account holder).

65. *See id.* (narrowly governing contents of electronic mail accounts rather than encompassing broader social media platforms).

66. *See* IND. CODE ANN. § 29-1-13-1.1 (West 2016) (explaining Indiana's law governing management and collection of digital account assets).

67. *Id.* § 1.1(b) (delineating requirement for custodian to provide personal representative access to electronically stored information).

68. *Id.* § 1.1(c) (lacking relevant definition of terms to provide guidance for executors).

69. *See id.* § 1.1(a) (omitting elaborative definitions of relevant statutory terms); Ray, *supra* note 58, at 604 (noting uncertainty regarding what type of digital assets Indiana's statute covers).

70. *See* IDAHO CODE ANN. § 15-5-424 (West 2015) (providing conservator authority over protected person's social networking website or email service); OKLA. STAT. ANN. tit. 58, § 269 (West 2016) (explaining authority vested in executor for social networking accounts under Oklahoma law).

71. IDAHO CODE ANN. § 15-5-424(3)(z).

72. *See* OKLA. STAT. ANN. tit. 58, § 269 (West 2016) (explaining authority vested in executor for social networking accounts under Oklahoma law). Specifically, Oklahoma's statute authorizes the executor or estate administrator to "take control of, conduct, continue, or terminate any accounts of a deceased person on any social networking website, any microblogging or short message service website or any e-mail service

account for TOS contracts—an omission that could render the Oklahoma law powerless based on uncertainty regarding whether authority belongs to the decedent's estate or, alternatively, ISPs.[73] Moreover, Virginia state law, before recent expansion, merely allowed parental access to a deceased minor's digital account material.[74]

Although state legislation governing this arena does exist, the spectrum of state protection of and authorization to digital property proves problematic.[75] First, inconsistencies exist regarding vested authority based on the type of fiduciaries at issue.[76] Second, although a minority of states enacted legislation governing digital account assets, the statutes vary greatly in scope.[77] Whereas some state statutes limit digital property management to email accounts, other statutes include management of social media, microblogging websites, and even information that a custodian stores electronically.[78] An additional layer of complication exists because many ISPs include choice-of-law clauses, creating further confusion as to which state's digital asset statute controls.[79] Courts enforce choice-of-law provisions so long as the provisions reasonably relate to the relevant transaction and are not void for public policy.[80]

D. Uniform Law Commission Suggests Model Legislation

Addressing ambiguities in the law governing digital assets through suggesting model state legislation that provides fiduciary rights over digital assets, the Uniform Law Commission created the UFADAA.[81] Primarily, the UFADAA seeks to enable fiduciary access to digital property in a way analogous to the manner in which fiduciaries access other types of property.[82] The UFADAA suggests states provide fiduciaries authorization to manage,

websites." *Id*.

73. *See* Ray, *supra* note 58, at 598-99 (noting uncertainty regarding what type of digital assets Oklahoma's statute applies to); *see also* Jason Mazzone, *Facebook's Afterlife*, 90 N.C. L. REV. 1643, 1676 (2012) (explaining substantial challenge to law's practical application based on contract law).

74. *See* VA. CODE ANN. §§ 64.2-109 to 110 (West 2016) (providing access to deceased minor's personal representative).

75. *See* Lamm et al., *supra* note 14, at 411 (explaining effects of inconsistent state legislation).

76. *See id.* (recognizing statutory variations based on type of fiduciaries). *Compare* IDAHO CODE ANN. § 15-5-424 (granting authority to conservators), *with* OKLA. STAT. ANN. tit. 58, § 269 (granting authority to personal representatives).

77. *See* Lamm et al., *supra* note 14, at 411 (explaining statutory fluctuations on what digital account types states cover and scope of protection).

78. *See id.* (noting inconsistent scope of state statutes managing digital property).

79. *See id.* at 412 (recognizing choice-of-law statutes create additional concern for fiduciaries).

80. *See* Cantu v. Jackson Nat'l Life Ins. Co., 579 F.3d 434, 437 (5th Cir. 2009) (framing validity inquiry of choice-of-law clause according to "reasonable relationship" to transaction).

81. *See* UNIF. FIDUCIARY ACCESS TO DIG. ASSETS ACT §§ 1-11 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 2014) (proposing uniform act to create fiduciary authority over digital accounts and assets).

82. *See id.*, prefatory n. (explaining UFADAA goal of removing barriers to fiduciary ability to access electronic accounts).

access, replicate, or eliminate digital property after death.[83] The UFADAA applies to conservators, trustees, and agents acting under a power of attorney, which extends application beyond mere personal representatives to include other important fiduciaries.[84] In providing access beyond personal representatives, the Uniform Law Commission sought to extend the class of people authorized to act on behalf of the digital account holder.[85] Moreover, the UFADAA's scope expands beyond any authority granted under existing state legislation.[86] The UFADAA strives to equip courts, ISPs, decedents, and fiduciaries with "certainty and predictability" in managing digital assets.[87]

In 2014, Delaware enacted the FADADAA, becoming the first state to

83. *See id.* (explaining purpose of empowering fiduciary to enter, control, or replicate digital account contents). Section 2 of the UFADAA provides relevant definitions for states, including parties relative to the scope of a fiduciary's authority, such as personal representative and trustee. *See id.* § 2. Importantly, Section 2 defines "[a]ccount holder" as "a person that has entered into a terms-of-service agreement with a custodian or a fiduciary for the person." *Id.* § 2(1). "Digital asset" is defined as "a record that is electronic," but excludes "an underlying asset or liability unless the asset or liability is itself a record that is electronic." *Id.* § 2(9). Further, Section 2 defines "[p]ersonal representative" as an "executor, administrator, special administrator, or person that performs substantially the same function under law of this state other than this [act]." *Id.* § 2(16).

84. *See id.*, prefatory n. (noting application to four distinct categories of fiduciaries). Section 3 considers the Act's applicability, detailing its relevant application to fiduciaries or agents, personal representatives, conservatorship proceedings, and trustees, while excluding application of an employer's digital asset used by an employee in regular business. *See id.* § 3.

85. *See* UFADAA, prefatory n. (distinguishing between fiduciary authority and unauthorized attempts to gain digital asset access). In Sections 4 through 7, the Uniform Law Commission grants authority in managing digital property to personal representatives, agents, trustees, and conservators. *See id.* §§ 4-7. Importantly, the UFADAA distinguishes between each fiduciary, with each receiving distinctive grants of authority in his or her uniquely recognized capacities. *See id.* More specifically, the model rule provides authority over a decedent's digital property to a personal representative in Section 4, but provides a requirement in Sections 5 and 6 for a specific grant of authority over digital property to an agent or conservator. *Compare id.* § 4 (recommending default power in personal representative), *with id.* §§ 5-6 (suggesting requirement for conservator and agent's specific allocation of authority by court). Section 5 concerns a conservator's access to a protected person's digital assets. *See id.* § 5. Although the specific provisions of Section 5 are modeled after Section 4, the Uniform Law Commission distinguishes the conservator from a personal representative in granting the court permissive discretion to grant a conservator a right to access. *See id.* Section 7 suggests bestowing authority over digital property held in trust to a trustee, requiring consistence with the relevant trust's governing terms. *See id.* § 7.

86. *See id.*, prefatory n. (recognizing issues in current state law's scope governing digital assets). UFADAA Section 4 discusses personal representative access to the decedent's digital accounts and assets. *See id.* § 4. Specifically, this section grants a personal representative of the decedent access to three specific categories of digital content. *See id.* First, UFADAA permits access to electronic communication content covered by the ECPA. *See id.* § 4(1). Additionally, UFADAA permits a personal representative access to "any catalogue of electronic communication" that the decedent sends or collects as well as any digital account that the decedent possessed or controlled upon death. *Id.* §§ 4(2)-(3). Consistent with the demands of federal law and the ECPA, in this section, UFADAA distinguishes between content discussed under the ECPA and the electronic logs and records ISPs release. *See id.* § 4 cmt.

87. *Id.*, prefatory n. The UFADAA promulgates guidelines for how a fiduciary attains ownership of, accesses, or copies a decedent's digital property. *See id.* § 8. Section 9 requires ISPs' compliance when considering fiduciary requests for accessing a decedent's digital property, while Section 10 provides immunity against civil liability for such service providers. *See id.* §§ 9-10. Finally, Section 11 calls for uniformity in the UFADAA's construction and application. *See id.* § 11.

replicate the proposed UFADAA.[88] Effective January 1, 2015, the law vests decedents' personal representatives, whose wills Delaware law governs, with the same authority as the account holder over digital assets.[89] With the passage of FADADAA, Delaware became the first state to enact broad legislation permitting family inheritance of digital assets in the same manner that they could inherit physical assets.[90]

E. Recent Developments

Based on the lack of clarity in the law governing ISPs, Internet companies have begun to take this issue into their own hands, directly addressing the treatment of digital assets postmortem.[91] For example, Google recently released a feature that provides users further options in managing the treatment of digital accounts after death, including an option to pass data along from their accounts to a designated representative.[92] Notably, through the recent creation of the "legacy contact" feature, Facebook similarly empowered users with a choice regarding the postmortem treatment of their social media account.[93] Although Facebook provided legacy contacts with significant account access, Facebook withheld access to an individual's private messages.[94] Additionally,

88. *See* DEL. CODE ANN. tit. 12, §§ 5001-07 (West 2015) (implementing FADADAA as Delaware law); *see also* Carney, *supra* note 10 (listing Delaware as first state to pass comprehensive legislation covering postmortem digital assets).

89. *See* Ross, *supra* note 12 (noting effect of Delaware law on digital property).

90. *See* Adam Clark Estes, *All States Should Adopt Delaware's Sweeping New Digital Inheritance Law*, GIZMODO (BLOG), Aug. 19, 2014, 2014 WLNR 22779512 (explaining breadth and comprehensiveness of Delaware's digital assets legislation).

91. *See* Geoffrey A. Fowler, *Google Lets Users Plan 'Digital Afterlife' By Naming Heirs*, WALL STREET J. (Apr. 11, 2013), http://blogs.wsj.com/digits/2013/04/11/google-lets-users-plan-digital-afterlife-by-naming-heirs/ (explaining Google's feature allowing users to plan digital afterlife through designating "Google heirs").

92. *See id.* (discussing Google's recent "Inactive Account Manager" feature). Google's feature, the "Inactive Account Manager," provides account users with a new choice to determine the fate of their account following their death. *See id.* Google allows users to delete all or a portion of their data from Gmail, Google+, cloud storage Drive, Picasa albums, YouTube, and other services after a certain period of inactivity. *See id.* Google also provided the option for users to grant access to one or more individuals following their death. *See id.* Google hopes the feature will allow its users to preserve privacy and stability in their account contents beyond death. *See id.*

93. *See* Damon Beres, *Facebook Just Made It Possible To Will Your Page to Someone When You Die*, HUFFINGTON POST (Feb. 12, 2015), http://www.huffingtonpost.com/2015/02/12/facebook-memorial_n_6669608.html [http://perma.cc/JUA9-3C57] (noting new Facebook feature allowing users to choose "legacy contact" to gain account access). This new feature gives users the option to choose an individual to gain control over certain aspects of his or her Facebook account after death. *See id.* Facebook also gives users the option to delete their account permanently after death. *See id.*

94. *See id.* (noting feature does not include access to decedent's private messages). Additionally, unlike an individual accessing a Facebook account with original login information, the legacy contact cannot edit or remove content that the decedent previously created. *See id.*; *see also What Is a Legacy Contact?*, FACEBOOK, https://www.facebook.com/help/1568013990080948 (last visited Mar. 29, 2016) [https://perma.cc/4XTC-49HQ]. Facebook defines a legacy contact as the person an account holder selects to attend to his or her account after "it's memorialized." *What Is a Legacy Contact?*, *supra*. A legacy contact's authorities include the ability to share a final message on the decedent's behalf, acknowledge new friend requests, and upload a

to date, twenty-seven states introduced legislation that tracks the language of the UFADAA.[95]

F. Prioritizing Privacy: States Turn Their Back to UFADAA

In the months following Delaware's implementation of a version of the UFADAA and many states attempting to follow suit, many states began to move in a different direction.[96] NetChoice—a trade organization that represents several ISPs and vehemently opposes the implementation of the UFADAA—drafted another version of model legislation governing digital assets postmortem.[97] This model legislation, PEAC, seeks to offer states draft legislation to provide fiduciary access to digital property following the death of an account holder.[98] Although the trend among states was originally toward advancing the UFADAA in their legislatures, versions of the original proposed bill have been denied in nearly every state since Delaware enacted it.[99] Support transpiring into opposition is likely due in part to technology companies' and NetChoice's staunch opposition to and advocacy against the UFADAA.[100]

PEAC takes a different approach than the UFADAA, claiming its primary motivation is protecting the privacy of individuals whose digital presence continues while they are no longer here physically.[101] For example, NetChoice cites a survey that claims more than seventy percent of Americans want privacy

new cover photo or profile picture for the deceased. *See id.*

95. *See Acts: Fiduciary Access to Digital Assets Act, Revised (2015)*, *supra* note 9 (tracking legislative acts introduced by states modeling UFADAA). The states beyond Delaware that considered or implemented versions of the UFADAA include: Alabama, Arizona, Colorado, Connecticut, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Maine, Maryland, Michigan, Minnesota, Mississippi, Nebraska, New Jersey, Oklahoma, Oregon, Pennsylvania, South Carolina, Tennessee, Utah, Washington, West Virginia, Wisconsin, and Wyoming. *See id.*; *see also* Rachel Emma Silverman, *When You Die, Who Can Read Your Email? A Controversial New Delaware Law Gives Executors More Access to Online Data*, WALL STREET J. (Feb. 1, 2015), http://www.wsj.com/articles/when-you-die-who-can-read-your-email-1422849600 (examining recent developments in state digital asset legislation). Those engaged in state government also speculate that additional states will consider passing similar laws that provide digital access. *See* Silverman, *supra.*

96. *See* Morgan M. Wiener, *Opposition to the Uniform Fiduciary Access to Digital Assets Act*, NAT'L L. REV., July 21, 2015, 2015 WLNR 21596160 (noting although twenty-six states introduced UFADAA legislation after Delaware, *none* of these bills passed).

97. *See id.* (explaining NetChoice went beyond mere opposition, setting forth original substitute to UFADAA).

98. *See Privacy Expectation Afterlife and Choices Act (PEAC)*, NETCHOICE, http://netchoice.org/library/privacy-expectation-afterlife-choices-act-peac/ (last visited Oct. 27, 2015) [http://perma.cc/D639-EZC2] [hereinafter *PEAC*] (outlining purpose of PEAC).

99. *See* Wiener, *supra* note 96 (noting states originally presenting versions of UFADAA have since opposed law).

100. *See id.* (explaining NetChoice's opposition to UFADAA, transpiring into its own version of fiduciary access legislation).

101. *See Privacy Afterlife: Empowering Users To Control Who Can See Their Online Accounts*, NETCHOICE, http://netchoice.org/library/decedent-information/ (last visited Mar. 29, 2016) [http://perma.cc/EFQ6-TJG8] (stating goal of allowing users to determine their own postmortem privacy).

in their Internet communications beyond death.[102] The group also argues that seventy percent of Americans feel "the law should err on the side of privacy when someone dies" without indicating his or her preference for treatment of digital property.[103] Additionally, the group cites studies to argue that Americans value privacy in the afterlife over ensuring familial access to digital property after losing a loved one.[104]

The goal of PEAC is twofold: seeking to promote efficient estate administration following the death of decedents while simultaneously striving to maintain privacy within decedents' digital property.[105] Section 1 of PEAC allows disclosure of information relating to decedent users' online accounts, pending the court makes several findings of fact.[106] Importantly, this section cross-references the SCA and prohibits a probate court from divulging communications or electronically stored content if disclosure violates that law.[107] Additionally, Section 1 governs whether ISPs must divulge information from a decedent's accounts.[108]

PEAC provisions also enumerate certain protections for ISPs.[109] PEAC

102. *See id.* (citing poll arguing Americans inordinately desire restraint over personal accounts, seeking privacy even beyond death).

103. *See id.* (explaining when decedent's intent unclear, law's treatment of digital communications should favor privacy).

104. *See id.* (claiming four out of five Americans prefer privacy over familial access upon death). The same study suggests merely fourteen percent of Americans believe the law should prioritize familial access regardless of the intent of the decedent and whether the decedent sought to maintain privacy within his or her online accounts. *See id.* Even further, the study proffers that forty-three percent of Americans believe that rather than allowing automatic access, ISPs should delete account content upon the decedent account holder's death. *See id.* The study suggests sixty-five percent of Americans believe it is against their privacy if online communications are shared with their family without their consent. *See id.*

105. *See PEAC*, *supra* note 98 (outlining purposes of and intent behind PEAC).

106. *See id.* §§ 1(A)(a)-(i) (allowing ISPs to divulge decedent account materials pending satisfaction of nine elements). The court must be persuaded that: the decedent account holder passed away; the decedent account holder subscribed to an ISP; the decedent's accounts have been recognized with particularity, incorporating an ISP-assigned "unique identifier"; no other users have authorization over the decedent's account; disclosure is consistent with the SCA's provisions; the disclosure request effectuates the goals of estate administration through narrowly tailored means; the executor or administrator demonstrates, in good faith, the relevance of account records to the resolution of monetary assets within the estate; the executor or administrator limits the request to content within one year before the decedent account holder's death; and the request is consistent with the decedent's intent as expressed in his or her will or testament. *Id.*

107. *See id.* § 1(A)(e) (noting judge must find disclosure does not violate Federal SCA "or other applicable law").

108. *See id.* §§ 1(B)(a)-(c) (requiring ISP disclosure pending executor or administrator satisfies three requirements). The provision compels disclosure insofar as the administrator or executor provides a request for the digital account contents in writing, a copy of the decedent account holder's death certificate, and the probate court's order. *See id.* Moreover, the court order must find either the decedent's will or an ISP product setting detailing how to treat account contents postmortem to demonstrate that the decedent expressly consented to the ISP's divulgement of stored communication. *See id.* § 1(B)(c)(i). The order must also require the estate to indemnify the ISP from both civil and criminal liability. *See id.* § 1(B)(c)(ii) (detailing provisions aimed at ensuring account content access consistent with decedent's intent and privacy concerns).

109. *See PEAC*, *supra* note 98 (detailing limitations on disclosure, which protect and lessen burdens on ISPs). For example, Section 2 provides an exception to Section 1 in circumstances involving an unreasonable

simultaneously purports to advance privacy protections for the decedent account holder.[110] Notably, Section 3 focuses on the decedent's intent, prohibiting a judge from compelling ISP divulgement if the decedent's intent demonstrates a desire for maintaining privacy in the communications.[111] Section 3 would exempt ISPs from compliance with PEAC Section 1 if the decedent manifested an intent to maintain privacy by deleting account contents while alive or utilizing an ISP's product setting to designate treatment of digital accounts postmortem.[112] Moreover, Section 3 provides for an exception where ISP divulgement would be inconsistent with other relevant laws.[113] Section 3 further limits the executor or administrator's rights in the decedent account holder's digital property—refusing to extend rights that exceed the original rights of the decedent account holder.[114] PEAC Section 4 allows time for current lawful users of existing accounts to object to divulgement and forbids disclosure if a user objects to disclosure within a reasonable time period.[115] Finally, PEAC Section 6 defines relevant terms used in the model legislation.[116]

G. Let's Try This Again: The Uniform Law Commission's Amended UFADAA

In a likely attempt to remedy the displeasure with the UFADAA amongst state legislatures, the Uniform Law Commission released an amended version of the law in 2015.[117] A more comprehensive version of the original model

hardship on ISPs, requiring courts to modify or quash an order if compliance would be overly burdensome, or if it does not fulfill each element of Section 1. *See id.* § 2. Section 5 clarifies that PEAC does not mandate that ISPs allow a party requesting access to take control over a decedent's account. *See id.* § 5. Section 7 protects an ISP from criminal or civil liability when the ISP exercises good-faith compliance with PEAC's provisions as implemented through a court order. *See id.* § 7.

110. *See id.* § 3 (enumerating provisions detailing safeguards preserving intent of decedent account holder).

111. *See id.* (noting decedent's intent should control, pending recognizable intent). For example, PEAC Section 3 interprets an account holder's action of deleting a certain account or its contents as expressing intent against disclosure. *See id.* Further, a decedent account holder's affirmative indication via a setting demonstrating a preference for content treatment over time signifies the decedent's intent to avoid disclosure. *See id.* This provision seems to cross-reference steps that ISPs, such as Facebook, have already begun to take in creating features that allow an account holder to designate an individual's access to account contents after the account holder's death. *See What is a Legacy Contact?*, *supra* note 94 (outlining legacy contact access to decedent's account).

112. *See PEAC*, *supra* note 98, § 3(a) (articulating specific ways decedent can express intent while living to prohibit divulgement when deceased). Alternatively, ISPs are likewise immune from Section 1's provisions if they possess knowledge of any manifestation of legal account access subsequent to the date of the decedent's passing. *See id.* § 3(b) (implying another user's lawful access takes precedence over estate administrator's request for information).

113. *See id.* § 3(c) (preventing disclosure when it would violate other laws).

114. *See id.* § 3 (confining scope of recipient rights in property). PEAC confers no more rights to the recipient than the original account holder. *Id.*

115. *See id.* § 4 (granting current account user period for objecting to disclosure where objection controls whether court discloses).

116. *See PEAC*, *supra* note 98, § 6 (defining relevant terms within PEAC).

117. *See* REVISED UNIF. FIDUCIARY ACCESS TO DIG. ASSETS ACT (UFADAA 2) (NAT'L CONFERENCE OF

law, the Revised Uniform Fiduciary Access to Digital Assets Act (UFADAA 2) modified several aspects of the Uniform Law Commission's original proposal.[118] UFADAA 2 also approaches several considerations regarding treatment of digital accounts postmortem—considerations neither the original UFADAA nor PEAC addressed.[119] UFADAA 2 also replicates ideas set forth in PEAC, which brings the act more in line with the decedent account holder's intent.[120]

UFADAA 2 expands upon important areas pertaining to fiduciary access from the original UFADAA, revising the consideration and effect of TOS contracts, for instance.[121] The original UFADAA made the effect of boilerplate language found within TOS contracts void against public policy, whereas UFADAA 2 engages in a three-pronged consideration of TOS contracts.[122] Under the revised standard, UFADAA 2 presents a hierarchal approach.[123] A decedent account holder's intent expressed via an online tool takes precedence over both an intent expression offline and TOS contracts pending the account holder's ability to modify or delete his or her direction at any time.[124] Next, a decedent account holder's intent directive regarding digital account contents treatment expressed in a trust or will, through power of attorney, or through another record, takes precedence over boilerplate contract language.[125] Finally, if the decedent account holder was silent, in that he or she did not indicate preference through any aforementioned method, the TOS contract dictates the outcome, unless it does not include a provision regarding fiduciary access.[126] Pending the TOS contract's silence on fiduciary access in circumstances where the decedent account holder did not provide direction via an online tool, will, trust, or other document signifying intent, other law controls.[127] Adding to the

COMM'RS ON UNIF. STATE LAWS 2015) (articulating new draft of UFADAA).

118. *See Comparison of the Uniform Fiduciary Access to Digital Assets Act (Original UFADAA), the Privacy Expectations Afterlife and Choices Act (PEAC Act), and the Revised Uniform Fiduciary Access to Digital Assets Act (Revised UFADAA)*, UNIFORM L. COMMISSION, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/Comparison%20of%20UFADAA%20PEAC%20and%20Revised%20UFADAA.pdf (last visited Oct. 27, 2015) [http://perma.cc/MGJ9-D3SD] [hereinafter *Uniform Law Comparison*] (detailing updates and changes made between original UFADAA and UFADAA 2).

119. *See id.* at 4-5 (comparing and contrasting various proposed UFADAA 2 provisions not addressed in either UFADAA or PEAC).

120. *See id.* at 4 (addressing deleted assets in same manner as PEAC by not requiring their disclosure). Although the original UFADAA did not address treatment of deleted assets, UFADAA 2 added a provision. *See id.*

121. *See id.* at 3 (noting distinctive treatment of garden-variety TOS contracts banning fiduciary access).

122. *See Uniform Law Comparison*, *supra* note 118, at 3 (reiterating differences between UFADAA 2 and original UFADAA regarding effect of TOS contracts).

123. *See id.*

124. *See id.*

125. *See id.*

126. *See Uniform Law Comparison*, *supra* note 118, at 3 (explaining three-pronged hierarchal approach to treating boilerplate contract language in fiduciary access context).

127. *See id.* (noting legal instruments indicating decedent intent when TOS contract lacks instruction).

unpredictability in this area of law, Virginia passed its own digital estate legislation, the Privacy Expectation Afterlife and Choices Act (VA PEAC), modeled after PEAC, which took effect on July 1, 2015.[128]

III. ANALYSIS

A. Concerns for Preemption: Room for States To Legislate in this Area?

Because the SCA prevents ISPs from turning over electronic account contents to any person or entity, at first glance, a state law granting broad fiduciary control over digital account contents seems misplaced and contrary to the federal government's prerogative.[129] In requiring ISPs to provide access to stored communications for fiduciaries, FADADAA and similarly drafted statutes may operate in direct contrast with the provisions of the SCA.[130] A cursory review of the circumstances surrounding this issue may lead a court to analogize a preemption concern for state digital asset estate legislation as akin to the situation in *Telecommunications Regulatory Board of Puerto Rico v. CTIA—The Wireless Ass'n*.[131] A court may reason that, like Puerto Rico's law requiring disclosure of information regarding telephone customers to the government, in requiring ISPs, such as social media providers, to grant broad access to stored communications, laws like Delaware's FADADAA compel ISPs to provide what the SCA expressly prohibits.[132] Because the SCA prohibits voluntary disclosure of electronic communications by RCS and ECS companies, FADADAA's requirement that "a custodian *shall* provide the

128. *See* VA. CODE ANN. §§ 64.2-109 to 115 (West 2016) (codifying model PEAC legislation into state's own digital asset law).

129. *See* 18 U.S.C. § 2702 (2012) (barring ISPs' divulgement of digital account content while such content held in their storage); *see also* Horton, *supra* note 30, at 569-70 (opining SCA bars ISPs from voluntarily disclosing digital account content postmortem); Borden, *supra* note 29, at 414 (arguing purpose and effect of SCA acts as bulwark to broad digital inheritance).

130. *Compare* 18 U.S.C. § 2702 (2012) (prohibiting ISPs' voluntary disclosure of electronically stored information), *with* DEL. CODE ANN. tit. 12, § 5005 (West 2015) (providing, upon fiduciary's written request, custodian *shall* provide access), *and* UFADAA § 8 (granting broad fiduciary access and control to decedent's digital assets and accounts).

131. *See* 752 F.3d 60, 61 (1st Cir. 2014) (holding SCA preempted Puerto Rico law requiring phone companies equip government with private information). The First Circuit held the express language of the SCA persuasive enough to resolve the preemption issue without needing to look to the SCA's legislative history. *See id.* at 66. Nonetheless, in considering the appellant's argument, the court considered the SCA's legislative history, concluding it "corroborates the congressional purpose made manifest by the statutory text." *Id.* Further, although the information that the Puerto Rican government sought was merely basic user details, such as names and phone numbers, rather than intimate or confidential conversations, the First Circuit still deemed the SCA's requirements satisfied. *See id.* at 66-67. Nevertheless, the court recognized that the SCA provides heightened protection to more private contents of communications while deeming even minimally intrusive subscriber information worthy of SCA protection from required disclosure. *See id.*

132. *See id.* at 68 (holding Puerto Rico's law directly conflicts with SCA); *see also supra* note 90 (explaining broad authority granted to fiduciaries under FADADAA).

fiduciary the applicable access" arguably creates an "irreconcilable conflict."[133]

Further, if the improbability of reading both statutes consistently based on their express language is unavailing, considering congressional intent behind the SCA may bolster the argument for a court to find preemption.[134] Granting broad fiduciary access to *all* types of communications seems counterintuitive to the SCA's express purpose, whereby Congress sought to provide Fourth Amendment-like privacy protections to Internet communications.[135]

Upon closer scrutiny, however, exceptions exist for the SCA's disclosure ban.[136] Although the SCA bars disclosure, disclosure may be appropriate when the account holder grants authorization by way of express consent.[137] In analyzing whether the SCA preempts state digital inheritance laws, the focus is on whether the state law at issue irreconcilably clashes with the SCA.[138]

To a greater extent than FADADAA, PEAC, which Virginia recently implemented and several other states are now considering, adheres to the SCA's requirements.[139] More specifically, PEAC is compatible with the SCA because, under both laws, determinations of disclosure turn on whether the account holder expressly consented to provide access.[140] Similarly, UFADAA 2 proves consistent with the SCA because rather than permitting fiduciary access in all circumstances, the model law seeks to effectuate the decedent

133. DEL. CODE ANN. tit. 12, § 5005(b) (West 2015) (emphasis added); Barnett Bank of Marion Cty., N.A. v. Nelson, 517 U.S. 25, 31 (1996).

134. *See supra* note 46 (describing preemption when state law obstructs purpose or intent of congressional action).

135. *See supra* note 28 and accompanying text (explaining SCA's purpose and effect of confined access to online stored communication, preserving information's privacy). Fourth Amendment jurisprudence does not currently protect ISP-held information because the private search doctrine confines protection to government action. *See* Kerr, *supra* note 28, at 1212. In empowering account holders with extensive privacy protections that prohibit ISP divulgement of stored communications, the SCA attempts to resolve this disparity. *See id.*

136. *See* 18 U.S.C. § 2702(b) (2012) (enumerating circumstances where ISPs' disclosure of account contents appropriate).

137. *See id.* § 2702(b)(3) (noting disclosure appropriate where account holder lawfully consents); *see also* 18 U.S.C. § 1030 (2012) (demonstrating congressional intent on punishing intentional access *without* authorization).

138. *See supra* notes 45-47 and accompanying text (detailing analytical framework for assessing preemption issues).

139. *Compare* 18 U.S.C. § 2702(b) (2012) (listing specific exceptions where ISPs empowered to disclose account contents), *with* DEL. CODE ANN. tit. 12, § 5004 (West 2015) (empowering fiduciary with authority over "any and all rights in digital assets and digital accounts . . . ."), *and PEAC*, *supra* note 98 (making required disclosure to executor or administrator exception rather than rule, requiring requisite user intent). PEAC specifically cross-references the SCA, requiring a judge to find disclosure of digital account contents consistent with the SCA. *See PEAC*, *supra* note 98, § 1(A)(e). Moreover, PEAC limits disclosure to circumstances consistent with the intent of the decedent account holder, necessitating express consent via will or a similar ISP feature that designates whether an account holder wishes to turn over account access. *See PEAC*, *supra* note 98, § 3(a).

140. *Compare* 18 U.S.C. § 2702(b)(3)(b) (2012) (allowing divulgement of stored electronic communication if originator provides lawful consent), *with PEAC*, *supra* note 98, § 3 (enabling disclosure of digital contents only upon sufficient indicia of account holder consent).

account holder's intent regarding disclosure.[141] Thus, although imperfect, both PEAC and UFADAA 2 provide potentially useful models for states seeking to implement digital asset legislation to achieve efficient and effective digital estate management, while simultaneously withstanding preemption challenges based on federal laws, such as the SCA and CFAA.[142]

B. Permitting Broad Fiduciary Access to Digital Communications Raises Unique Privacy Concerns

In providing broad fiduciary access in an analogous manner to tangible physical property, FADADAA, and similar sweeping state legislative endeavors, fail to consider the undoubtedly private or intimate nature of certain types of digital property.[143] Such a broad approach that categorically grants access and control to fiduciaries, although well-intentioned, may cast aside the intent of the decedent account holder, which, depending on the content or nature of the digital property, may be to restrict fiduciary access in the interest of privacy.[144]

For example, based on the potentially intimate details contained within a decedent's email or private Facebook message, allowing broad fiduciary access raises similar privacy concerns as addressed in the case of *Viacom International, Inc. v. YouTube Inc.*[145] Similar to a YouTube user that constricts public access to her videos through adjusted privacy settings, by specifically addressing a message to a particular recipient in an email or Facebook message, an individual takes steps to protect, or at least section off, her communications from the public.[146] Applying the court's reasoning in *Viacom International* to the context of an email, in choosing to convey information through email, rather than a more public platform, the decedent account holder elects to share

141. *See supra* note 120 and accompanying text (noting UFADAA 2 focuses on intent of decedent account holder in determining appropriateness of access).

142. *See PEAC*, *supra* note 98, § 1(A)(e) (incorporating reference to SCA and other relevant law in provision); *supra* text accompanying notes 126-127 (implicitly referencing SCA by measuring decedent account holder intent in analyzing digital account treatment).

143. *See* DEL. CODE ANN. tit. 12, § 5002(7) (West 2015) (providing scope of FADADAA and defining term "[d]igital asset"). Delaware broadly defines "[d]igital asset[s]" to include private and confidential information including "codes, health care records, health insurance records, . . . [and] usernames and passwords . . . ." *Id.* The types of information that a fiduciary is enabled to access through FADADAA are nearly limitless, as the law seems to pay no regard to the potentially personal and private nature of much of this information. *See id.* FADADAA also seems to ignore the SCA's prohibitions on ISPs, which limit the ability of ISPs to voluntary disclose communications to anyone. *Compare* 18 U.S.C. § 2702 (2012), *with* DEL. CODE ANN. tit. 12, § 5004.

144. *See* DEL. CODE ANN. tit. 12, § 5004 (allowing fiduciary access to digital content regardless of type of content or privacy settings); *see also supra* notes 102-104 (prioritizing preservation of private nature of online communications over encouraging familial access).

145. *See supra* note 38 and accompanying text (describing privacy concerns arising during disclosure of private YouTube videos).

146. *See supra* note 38 and accompanying text (emphasizing steps user takes to limit public access to videos in privacy analysis).

personal information with only "specified recipients."[147] An analogy using Facebook further demonstrates that in choosing to communicate through a private message to a designated individual, rather than posting information publicly on a Facebook wall, the decedent account holder purposefully constrains public access, which arguably should include family member or heir access.[148] Requiring blanket disclosure of all digital property, regardless of the confidential nature of the information contained within, raises serious privacy concerns.[149]

C. Preserving Privacy Requires Disclosure Faithful to Decedent Account Holder's Intent

The spirit and thrust of the SCA and CFAA suggest state digital asset legislation should account for the unique privacy concerns underlying Internet communications.[150] To this end, PEAC offers an effective rubric for states to implement digital asset legislation with privacy interests at its core.[151] More specifically, PEAC appropriately sets a high threshold for a judicial determination permitting disclosure by proposing a rebuttable presumption against disclosure—a standard erring on the side of maintaining the private nature of electronic accounts.[152] Moreover, rather than presume intent to disclose, by requiring express consent, PEAC faithfully recognizes the inherently private nature of online communications, while permitting disclosure when consistent with the decedent account holder's intent.[153]

Further, PEAC provides a pragmatic and contemporary approach, which incorporates by reference tools that electronic service providers—such as Facebook with the legacy contact feature—have provided to gauge user intent before death.[154] Heightened recognition of real privacy interests is apparent in PEAC's incorporation of current features to decipher intent because such

147. *See* 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (noting significance of having specified recipients in determining whether ECPA should prevent disclosure).

148. *Cf. supra* note 38 and accompanying text (noting importance of user limiting audience of online communication in deciphering intent for disclosure).

149. *See supra* notes 102-104 and accompanying text (discussing privacy concerns associated with broad disclosure of private online communications).

150. *See supra* notes 28-29 and accompanying text (summarizing congressional intent to ensure privacy protections in modern digital communications through ECPA).

151. *See supra* note 101 and accompanying text (highlighting PEAC's core purpose to maintain private nature of digital communications beyond death).

152. *See supra* note 108 and accompanying text (detailing elemental test for disclosure, requiring judge convinced of nine factors).

153. *See supra* notes 110-111 and accompanying text (offering guidelines to advance privacy concerns of decedent account holder).

154. *See PEAC*, *supra* note 98, § 3(a) (detailing PEAC section, which defers to user intent through affirmative indication in account setting); *see also* Fowler, *supra* note 91 (discussing Google feature empowering users to designate account manager for account after death); *What Is a Legacy Contact?*, *supra* note 94 (explaining Facebook feature allowing user choice of who controls account after death).

features narrowly confine the scope of access granted to a designated individual.[155] Notably, for example, the authority vested in a legacy contact on Facebook is restricted—such individuals are not permitted access to private messages, nor can they edit or remove previously created content.[156] Additionally, in attempting to preserve and decipher the wishes of a deceased user, PEAC prudently recognizes a decedent account holder's action of deleting account contents while alive as symbolizing an intent to prevent disclosure after death.[157]

IV. CONCLUSION

Although states have begun making progress in passing and considering comprehensive digital asset legislation, the law's treatment of postmortem digital assets remains unclear. Further, a court ruling is likely necessary to address the intersection of state and federal law concerning the handling of digital property postmortem. Such a ruling is particularly necessary with regards to whether the SCA effectively preempts the impact of state laws requiring ISPs to turn over a decedent account holder's digital property.

With the increased prevalence and role of online accounts in our daily lives, it will be important for a court to consider whether we carry an expectation of privacy in such online property and communications to the grave. A court choosing to take up the issue will confront the difficult conflict between a family's interest in maintaining memories of their loved ones through preserving their online life and the decedent account holder's countervailing interest in maintaining the privacy of intimate or controversial online information. A balanced approach is attainable, and PEAC provides a useful framework for states to achieve effective digital estate management while preserving the privacy interests of the decedent account holder.

Matthew W. Costello

155. *See supra* notes 93-94 (delineating limited authority of individual selected as legacy contact).

156. *See supra* note 94 and accompanying text (discussing limited authority and access of legacy contact when taking over deceased user's account).

157. *See PEAC*, *supra* note 98, § 3(a) (noting action of removing account contents while alive instructive as to intent after death).