University of Miami Law Review

Volume 68
Number 2 *Volume 68 Number 2 (Winter 2014)*
SYMPOSIUM: Social Media and the Law

Article 10

1-1-2014

Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act

Samantha D. Haworth

Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act

SAMANTHA D. HAWORTH*

INTRODUCTION

On July 27, 2012, a teenage girl named Alison Atkins passed away from colon disease.[1] Her family turned to her online accounts for consolation and answers.[2] The family had to circumvent the teen's computer password and use her computer's automatic log-in function to access Alison's Twitter, Facebook, Tumblr, and email accounts.[3] Alison's online accounts contained conflicting characterizations of her life—

* Articles and Comments Editor, *University of Miami Law Review*; J.D. Candidate 2014, University of Miami School of Law; B.S. 2009, University of Florida. This Note is dedicated to my amazing and supportive husband, parents, family, and friends. A special thank you to Professor Kunal Parker for his guidance throughout my work on this Note. I am also grateful to Joshua Plager and the *University of Miami Law Review* for their feedback during the editing process.

1. Geoffrey A. Fowler, *Life and Death Online: Who Controls a Digital Legacy?*, WALL ST. J. (Jan. 5, 2013, 7:30 AM), *available at* http://online.wsj.com/article/SB10001424127887324677204578188220364231346.html. Although the Atkins case occurred in Canada, the issues surrounding her digital estate are analogous to those facing American families.

2. *Id.*

3. *Id.*

happy family pictures and dark, private journals.[4] Whether Alison wanted her online life viewed after her death was unknown. Nevertheless, the family's control over these accounts was fleeting, as the accounts eventually logged out or got deleted, and the contents were lost forever.[5]

When Internet users die without planning for their digital lives, families and estate executors are left to guess the users' wishes. Families may violate terms of service agreements and battle with Internet service providers to access digital property that the deceased never wanted others to access. Discussing the Atkins family, journalist Geoffrey A. Fowler wrote, "[T]aking hold of Alison Atkins's digital afterlife forced her family to tread a line between celebrating her, and invading her privacy. In the process, her family discovered some dark journals Alison clearly meant to conceal. 'She had passwords for a reason.'"[6]

Handling digital assets after death presents numerous practical, legal, and moral problems. Accounting for all of one's assets and rounding up the requisite passwords comprise the first step to managing a digital estate.[7] Professors Gerry W. Beyer and Naomi Cahn suggest drafting a separate document to supplement a will with log-in information to protect the testator's privacy because probated wills become public record.[8] Beyer and Cahn suggest designating how each asset should be handled, such as which assets should be deleted and which ones should be kept and by whom.[9] This approach is helpful in accounting for all of one's property, but it does not fully address how a family member or personal representative of an estate can implement these wishes legally.

This Note will explore the world of digital assets and how legislation can ensure the proper disposition of decedents' online selves. Part I explores the different kinds of digital assets and how courts deal with these assets in multiple types of litigation. Part II discusses the legislative solutions currently in place and under consideration for handling digital assets at death. Part III analyzes the Proposed Uniform Fiduciary Access to Digital Assets Act and discusses its innovations and shortfalls. Part IV examines what types of control fiduciaries should be allowed to

4. *Id.*

5. *Id.*

6. *Id.*

7. *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, 315–18 (2011).

8. Gerry W. Beyer & Naomi Cahn, *When You Pass on, Don't Leave the Passwords Behind: Planning for Digital Assets*, 26 PROB. & PROP. 40, 42–43 (2012).

9. *Id.*

exercise over digital assets. Finally, this Note will conclude with recommendations on how to best improve the Uniform Act.

I. DIGITAL ASSETS AS PROPERTY

A. *Defining Digital Assets*

Defining what constitutes a digital asset is no easy task. New Internet uses are constantly created. Any definition of digital assets needs to be broad enough to evolve with online innovation and clear enough for lawyers, online service providers, and the general public to understand what is included under the definition. A working definition of a digital asset, in a general sense, is

> a) information created, generated, sent, communicated, received, or stored by electronic means on a digital device or system that delivers digital information, and includes a contract right; and b) an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information which the account holder is entitled to access.[10]

Email and Facebook accounts are some of the more recognizable types of property meeting this definition, but others include online bank accounts, deleted blogs, dating profiles, and psychic reading transcripts. Creating categories of property that meet the "digital assets" definition is necessary for drafting comprehensive legislation that properly addresses all digital assets. This author proposes dividing digital assets into four categories: (1) Access Information, (2) Tangible Digital Assets, (3) Intangible Digital Assets, and (4) Metadata.

(1) Access Information: Account numbers and log-in information should be left to an executor to ensure an orderly distribution of digital property. However, the access information is often separate from the property it protects. Attorney David M. Lenz described access information as not an "asset" in and of itself, but rather as a means to accessing other assets.[11] For example, a log-in password to an E-Trade account makes accessing the underlying investments easier. Testators will bequeath the investment itself, not the log-in information.

(2) Tangible Digital Assets: This category includes photographs, PDFs, documents, emails, online savings account balances, domain names, and blog posts. Tangible assets are not tangible in the physical sense; they are compositions or property that hold a definable form.

---

10. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 2 (Proposed Discussion Draft Oct. 22, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013nov_FADA_Mtg_Draft.pdf. *See* discussion *infra* Part III.

11. David M. Lenz, *Death and Downloads: The Evolving Law of Fiduciary Access to Digital Assets*, 23 OHIO PROB. L.J. NL 2 (2012).

These are likely files that can be named and transferred to another. Tangible digital assets can likely be converted into physical assets, such as printing a picture or receiving a check for the value of an online savings account. These assets may have financial, cultural, or sentimental value, and these assets will define the bulk of digital property that a deceased's survivors will seek out.

(3) Intangible Digital Assets: This category is harder to conceptualize than tangible digital assets. Intangible assets are "likes" on Facebook, website profiles, and comments or reviews left on a blog. Internet users can have intangible assets spread over cyberspace in volumes. Testators may plan for pictures kept online but forget to plan for the information posted on a dating profile. As more and more people use the Internet and smartphones to conduct business and leisure activities, they leave a trail of thumbs up and thumbs down across cyberspace. Intangible assets will likely need to be deleted or shut down.

(4) Metadata: Metadata consists of data electronically stored within a document or website about the data's access history, location tags, hidden text, author history, deleted data, code, and more.[12] Most websites collect this information every time an Internet user clicks on a link.[13] These assets often leave a trail to every website a person visited online. This last category builds off of the logic and problems with intangible assets, except this type of information is even more obscure and may not even be accessible to testators themselves. Metadata often goes overlooked. While many survivors of a deceased loved one have no interest in this type of information, it can be invaluable to others—such as those trying to cope with a tragic death or those initiating wrongful death litigation.

B. *Digital Assets in Litigation*

Reported case law on how these different types of digital assets are accessed and distributed through the probate system is nearly nonexistent at this time. However, it is helpful to consider discovery motions in civil litigation to see a clearer picture of what kinds of digital property exist in cyberspace and why people want this property. Many jurisdictions now allow discovery of social networking websites in civil lawsuits.[14] In *Glazer v. Fireman's Fund Insurance Co.*, a magistrate judge

12. *See* Joseph Capobianco & Gabrielle R. Schaich-Fardella, *Electronic Age Changes in Legal Practice, Which No Attorney Can Ignore*, 84 N.Y. ST. B.J. 30, 31 (2012).

13. For example, Yahoo!'s Privacy Policy provides that "Yahoo automatically receives and records information from your computer and browser, including your IP address, Yahoo cookie information, software and hardware attributes, and the page you request." *Yahoo Privacy Policy*, YAHOO!, http://info.yahoo.com/privacy/us/yahoo/ (last updated May 31, 2013).

14. *See, e.g.*, Ledbetter v. Wal-Mart Stores, Inc., No. 06-CV-01958-WYD-MJW, 2009 WL

ordered a plaintiff to turn over transcripts of her online conversations with a psychic during discovery in an employment discrimination suit.[15] In the probate context, a federal court ordered the estate of a woman who died in an airplane crash to produce all of the deceased woman's social media accounts, emails, text messages, and instant messages that related to the decedent's domicile and the estate's loss of support claims.[16]

Parties seek metadata during discovery with increasing regularity, particularly when the timetable of events is central to the dispute. It is also sought when a party fears that another party "cleaned up" his online presence and deleted digital information before it was requested in discovery. In New York, a judge ordered a plaintiff to give the defendant "access to [the p]laintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information."[17] The defense won this extensive access after the public portions of the plaintiff's Facebook and MySpace pages contained information contradicting the plaintiff's personal injury claims.[18] In a Delaware case, a judge granted a motion to compel document requests in native format with the original metadata when "the integrity of dates entered facially on documents authorizing the award of stock options [was] at the heart of the dispute."[19] In a New York copyright infringement suit, a judge compelled production of all data showing when certain YouTube videos were viewed.[20]

C. *Which Digital Assets Are Worth Protecting at Death?*

A major question remains after determining what digital assets are floating out in cyberspace: Are these assets important and worth protect-

---

1067018, at *4 (D. Colo. Apr. 21, 2009), *available at* http://docs.justia.com/cases/federal/district-courts/colorado/codce/1:2006cv01958/98669/179 (denying motion for protective order to block discovery of social networking sites because the request was "reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues"); Largent v. Reed, No. 2009-1823, 2011 WL 5632688, at *13 (Pa. Ct. Com. Pl. Nov. 8, 2011), *available at* http://www.theemployerhandbook.com/Largent.pdf (holding that no general privacy right exists to shield Facebook posts from discovery). *But see* Keller v. Nat'l Farmers Union Prop. & Cas. Co., No. CV 12-72-M-DLC-JCL, 2013 WL 27731, at *4–5 (D. Mont. Jan. 2, 2013) (limiting discovery to a list of social networking sites subscribed to because the defendant did not provide evidence that the sites would have information that undermined the plaintiffs' claims).

15. Glazer v. Fireman's Fund Ins. Co., No. 11 Civ. 4374(PGG)(FM), 2012 WL 1197167, at *5 (S.D.N.Y. Apr. 5, 2012).

16. *In re* Air Crash Near Clarence Ctr., N.Y., on Feb. 12, 2009, No. 09-CV-961S, 2011 WL 6370189, at *6 (W.D.N.Y. Dec. 20, 2011). The deceased's domicile was important to the case, as it determined whether Chinese or New Jersey law applied.

17. Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010).

18. *Id.*

19. Ryan v. Gifford, No. 2213-CC, 2007 WL 4259557, at *1 (Del. Ch. Nov. 30, 2007).

20. Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256, 265 (S.D.N.Y. 2008).

ing at death? The answer is yes and no. Intangible digital assets should not be viewed as property belonging to each individual testator unless a contractual agreement says otherwise. We leave our footprints everywhere we go in the physical world. We sign guest books at museums and hotels. We give our business cards to acquaintances at conferences. We leave details with our dry cleaners on how we like our shirts pressed. These little bits of personal information are left every place we go. Yet, until now, we have not thought of that information as an asset belonging to each individual. Guest books and rolodexes belong to the businesses and people we leave them with. The problem with the online world is that suddenly the Internet versions of this information, such as "likes" and profiles, are all across the Web and are easily searchable and easily disseminated.

The changing availability of these small bits of personal information is creating a stir. However, ownership of the information should not change just because it is more accessible. Many physical businesses that offer services or products that are secretive and otherwise embarrassing are likely under no legal obligation to protect that information in real life. For example, hotels used for affairs or adult video stores likely keep client information private for customer loyalty purposes and not because they have a legal duty to not identify people who patronize their businesses. Intangible digital assets should be treated at death as client information collected by physical businesses. Therefore, no statutory protection should be required for these types of assets at death. Rather, they should be available for access by subpoena as discussed above with discovery litigation.

The only exception should be for metadata on one's own computer and documents or log-in histories that the testator took steps to erase during life. In the tangible world, unsent letters could be torn up and discarded. But in the digital world, draft emails can never really be erased forever. The line between metadata of personal deleted works and metadata that belong to the recipient or business entity is a gray one. However, as law on the relatively new concept of metadata evolves, understanding how to handle it at death will evolve as well.

Tangible digital assets should be handled differently. These assets can involve great sums of money and priceless cultural works. As these assets are more definable, their potential value warrants statutory attention. It is worth state legislatures' time and energy to provide protection for the ownership and use of testator's tangible digital assets after death.[21] Access information is the necessary key to tangible digital

21. *See* discussion *infra* Part IV and Conclusion (discussing the kinds of protections that should be available for tangible digital assets).

assets, and it should be treated how keys to lock boxes and titles to cars are treated in the physical world.

II. STATE STATUTES

Five states have enacted legislation specifically allowing personal representatives to access certain types of a deceased's digital assets.[22] Rhode Island's and Connecticut's statutes give executors access to or copies of the contents of email accounts.[23] Idaho's and Oklahoma's statutes allow for estates to "take control of, conduct, continue or terminate any accounts of the decedent on any social networking website, any microblogging or short message service website or any e-mail service website."[24] Nebraska has proposed similar legislation.[25] Indiana's statute does not specifically outline the types of online information subject to the statute.[26] Rather, it requires a custodian of electronically stored information to provide the personal representative with access to or copies of "any documents or information of the deceased person stored electronically by the custodian."[27] This language is significantly broader than the language in the other four enacted statutes and can likely grow as the types of digital assets that decedents use grow.

In 2013, Oregon proposed legislation with even more progressive language than any other enacted statute.[28] Oregon proposes allowing access, control, and disposal of "any digital assets and digital accounts."[29] The proposed legislation requires a "custodian of digital accounts and digital assets to transfer, deliver or provide access to accounts or electronic copies of assets to [a] personal representative, conservator or settlor upon written request."[30] If enacted, Oregon would be the first state to use the term "digital assets" in a statutory context.

---

22. CONN. GEN. STAT. § 45a-334a (2012); IDAHO CODE ANN. § 15-3-715(28) (2012); IND. CODE § 29-1-13-1.1 (2012); OKLA. STAT. tit. 58, § 269 (2012); R.I. GEN. LAWS § 33-27-3 (2012).

23. CONN. GEN. STAT. § 45a-334a; R.I. GEN. LAWS § 33-27-3.

24. IDAHO CODE ANN. § 15-3-715(28); OKLA. STAT. tit. 58, § 269.

25. L.B. 738, 102d Leg., 2d Reg. Sess. (Neb. 2011).

26. IND. CODE § 29-1-13-1.1.

27. *Id.*

28. S.B. 54, §2(26) 77th Leg., Reg. Sess. (Or. 2013).

29. S.B. 54.

30. The above quote is a summary by the bill's editor. S.B. 54 provides as follows:

> (13) "Digital accounts" includes, but is not limited to, electronic mail, financial, personal and other online accounts.
>
> (14) "Digital assets" includes, but is not limited to, text, images, multimedia information or other property stored in a digital format, whether stored on a server, computer or other physical device or in an electronic medium, regardless of the ownership of the physical device or electronic medium in which the digital asset is stored. "Digital assets" includes, but is not limited to, words, characters, codes or contractual rights necessary to access the digital assets.

Two other states have enacted laws addressing issues with digital assets in other contexts. Delaware allows an agent authorized under a personal power of attorney to access communications and communicate electronically on behalf of a living principal.[31] However, Delaware does not have a similar statute that expressly authorizes such access to electronic communications after the principal's death. California has a statute requiring email service providers to provide a thirty-day notice to users before permanently deleting their email accounts.[32] While this statute is not limited to accounts terminated upon the death of the account holder, the statute helps notify and give time to surviving family members of email account holders to take action and retrieve emails before they are lost forever.

III. ANALYZING THE UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

A. *Applicability*

The Uniform Law Commission, which produces the Uniform Probate Code and numerous other Model and Uniform laws, has been called to guide the formulation of uniform state legislation to address the disposition of digital assets at death.[33] On January 21, 2012, the Uniform Law Commission's Executive Committee approved a resolution to form a Study Committee to research the "need for and feasibility of state legislation on fiduciary powers and authority to access digital information."[34] A Drafting Committee ("Committee") has since been formed, and it released a discussion draft of a Proposed Uniform Fiduciary Access to Digital Assets Act ("FADAA Draft") on January 18, 2013.[35] The FADAA Draft was recently updated on October 22, 2013.[36] The current proposal is still in the drafting stage and will need to be submitted for debate before the entire Uniform Law Commission at a minimum

31. DEL. CODE ANN. tit. 12, § 49A-203(9) (2012).

32. CAL. BUS. & PROF. CODE § 17538.35(a) (2012).

33. *See* Tyler G. Tarney, Comment, *A Call for Legislation to Permit the Transfer of Digital Assets at Death*, 40 CAP. U. L. REV. 773, 797–98 (2012).

34. UNIF. LAW COMM'N, MINUTES OF THE MIDYEAR MEETING OF THE COMMITTEE ON SCOPE AND PROGRAM 11 (Jan. 20, 2012), *available at* http://www.uniformlaws.org/ shared/docs/scope/ScopeMinutes_012012.pdf.

35. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (Proposed Discussion Draft Jan. 18, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jan18_FADA_MtgDraft.pdf.

36. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (Proposed Discussion Draft Oct. 22, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013nov_FADA_Mtg_Draft.pdf.

of two annual meetings once complete.[37] It then must be approved by the Committee of the Whole, and a minimum of twenty states must approve the Act before it becomes an official Uniform Act.[38] Once an official Uniform Act, individual states must choose to enact the statute wholly or partially. Thus, the draft is a long way from becoming binding authority, but it provides a helpful model for other states looking to draft their own legislation. It also provides a much more comprehensive look into the statutory and implementation issues of statutes handling digital property than any of the state laws currently in effect.[39]

The FADAA Draft seeks to "vest fiduciaries with the authority to access, manage, distribute, copy or delete digital assets and accounts."[40] The draft expands beyond personal representatives to conservators, agents acting under a power of attorney, and trustees.[41] The multiple types of fiduciaries covered under the Act are logical and more efficiently address all of these fiduciary interests at once.

The first major component of the FADAA Draft is the definitions of the terms used within it.[42] As many of these terms have never before been defined in any statutes, the Committee must carefully craft definitions without much guidance. The Committee must specifically make its definitions comply with federal and state laws dealing with unauthorized access to digital information.[43] The Stored Communications Act ("SCA") makes it a crime for anyone to intentionally access electronic communications without proper authorization.[44] The punishment for individuals who violate the SCA can be up to five years imprisonment

37. ULC Drafting Process, UNIF. LAW COMM'N, http://www.uniformlaws.org/Narrative.aspx?title=ULC%20Drafting%20Process (last visited Dec. 29, 2013).

38. *Id.*

39. *See* CONN. GEN. STAT. § 45a-334a (2012); IDAHO CODE ANN. § 15-3-715(28) (2012); IND. CODE § 29-1-13-1.1 (2012); OKLA. STAT. tit. 58, § 269 (2012); R.I. GEN. LAWS § 33-27-3 (2012).

40. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT prefatory note (Proposed Discussion Draft Oct. 22, 2013).

41. *Id.*

42. *Id.* § 2.

43. *See, e.g.*, 18 U.S.C. §§ 2701–2711 (2012); 18 U.S.C. § 1030 (2012). For a compilation of state unauthorized access laws, see *Computerized Hacking and Unauthorized Access Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (May 21, 2009), http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx, *noted in* UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 8 cmt.

44. 18 U.S.C. § 2701(a) reads as follows:

> (a) Offense.—Except as provided in subsection (c) of this section whoever—
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility;
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

and fines.[45] Under 18 U.S.C. § 2702, custodians of information are prohibited from releasing online communications without proper authorization.[46] Electronic communication custodians are included under the SCA if they function as an electronic communication service ("ECS") or a remote computing service ("RCS").[47] A provider falls under ECS if it allows users to send or receive wire or electronic communications,[48] and it falls under RCS if it provides "computer storage or processing services by means of an electronic communications system."[49] This distinction is important because it determines what level of privacy is attached to that communication.[50] Whether an online service provider like Facebook falls under the SCA and is exposed to liability for unauthorized disclosures differs based on the particular type of communication disclosed and whether it is deemed an ECS or RCS provider. ECS and RCS providers can disclose protected communications with "lawful consent."[51]

The case law on which websites and providers are or are not covered under the SCA is just now developing. A United States district court in California held that private messaging through a webmail service or through a social networking site falls under the protection of the SCA.[52] Twitter has also been held to be an electronic communication

45. 18 U.S.C. § 2701(b)(2).

46. *Id.* § 2702.

47. 18 U.S.C. § 2702 reads as follows:

> (a) Prohibitions.—Except as provided in subsection (b) or (c)—
>
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; . . . .

48. 18 U.S.C. § 2510(15) (2012).

49. *Id.* § 2711(2).

50. For a more comprehensive analysis of the SCA and the distinctions between ECS and RCS, see Allen D. Hankins, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295, 299–300 (2012).

51. 18 U.S.C. § 2702(b)(3) (2012).

52. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010); *see also* In Re Request for Order Requiring Facebook, Inc. to Produce Documents and Things, No. C 12-80171 LHK (PSG) (N.D. Cal. Sept. 20, 2012), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/5:2012mc80171/257305/22/0.pdf?ts=1348220335 (quashing a

provider under the SCA.[53] Other rulings have been less clear-cut. Some cases turn on subtle distinctions based on how digital information was stored or what types of privacy settings were attached to the data. In New York, YouTube videos saved as private were protected under the SCA, but public videos later removed were not.[54] The Court of Appeals for the Ninth Circuit held that email messages stored on a server were protected under the SCA.[55] In South Carolina, a court ruled, "[w]e decline to hold that retaining an opened email [that was not downloaded or otherwise saved] constitutes storing it for backup protection under the [Stored Communications] Act."[56]

The complexities of the SCA may make Internet service providers wary to release information. Both individual fiduciaries and service providers are dancing around the contours of the SCA's provisions in order to avoid any liability for violating the SCA. 18 U.S.C. § 2702 allows disclosure "with 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."[57] This language does not specifically provide for consent given by a fiduciary or assignee. Thus, the language proposed in the FADAA Draft must be specifically written to address compliance with the SCA and other unauthorized access laws.[58, 59] In order to ensure compliance, the Committee drafted its fiduciary authority section to mirror the language of the SCA and maintain that fiduciaries have the same authority to access information as the originator or account holder.[60]

Section Three of the FADAA Draft limits the Act's applicability to grants of authority given to a fiduciary.[61] The cases of family members fighting for access to emails of deceased loved ones that have made headlines in recent years[62] would not be covered under this Act because

---

subpoena for Facebook records requested by a family seeking information to prove that its daughter did not commit suicide because the subpoena violated the SCA).

53. People v. Harris, 945 N.Y.S.2d 505, 511 (N.Y. Crim. Ct. 2012).

54. Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256, 265 (S.D.N.Y. 2008).

55. Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004).

56. Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012).

57. 18 U.S.C. § 2702(b)(3) (2012).

58. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 4(a)(3). (Proposed Discussion Draft Oct. 22, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013nov_FADA_Mtg_Draft.pdf.

59. For example, fiduciaries also have to contend with the Computer Fraud and Abuse Act, which prohibits intentional unauthorized access to computers. 18 U.S.C. § 1030(a)(2) (2012).

60. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 8(a), 8 cmt.

61. *Id.* § 3.

62. *See, e.g.*, Michael Avok, *States Tackle Legislation Giving Kin of Dead Facebook Users Access to Digital Legacies*, DENVER POST (Mar. 16, 2012, 2:52 AM), http://www.denverpost.com/business/ci_20185040/states-tackle-legislation-giving-kin-dead-facebook-users; Jessica Hopper, *Digital Afterlife: What Happens to Your Online Accounts When You Die?*, ROCK CENTER (June 1,

"their efforts are subject to other laws."[63] It is unclear what "other laws" the Committee refers to here. All the state statutes currently in effect on the issue also give access of covered digital property only to an executor or administrator of an estate.[64] This creates certain practical issues for families seeking prized emails, photos, or documents of loved ones. A will likely needs to specifically give access to family members, and the will needs to be probated to grant the authority to a personal representative to access digital property. For example, a young man who dies unexpectedly may have no assets to probate. If the young man's parents want to access his pictures on Facebook, under a plain reading of this Act, the parents would have to engage in court proceedings first.[65]

Requiring a formal estate to be established also creates problems for those with claims against a decedent's digital property. In *Davis v. Google*, a blogger posted an allegedly defamatory statement about the mother of a famous speed skater.[66] The blogger then passed away, and he had no estate against which Davis could seek relief.[67] Davis had to seek a court order compelling Google, the host company of the blog, to take down the post, but Google claimed that it did not have control over customers' posts.[68] This unfortunate situation would not be resolved by the current FADAA Draft because a fiduciary needs a grant of authority recognized by the Act for the blog post to be taken down. The *Davis* case highlights an important point: Legislation to address the disposition of digital property will only work if wills are made and estates are probated. This leaves a gaping hole in the resolution of the digital assets conundrum.

B. *Establishing Authority*

The central purpose of the FADAA Draft is to vest authority in fiduciaries to control digital property.[69] There are two main concepts in this goal that require analysis: how to get the authority and how to exer-

---

2012, 10:53 AM), http://rockcenter.nbcnews.com/_news/2012/06/01/11995859-digital-afterlife-what-happens-to-your-online-accounts-when-you-die.

63. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 3 cmt ("Family members or friends may seek such access, but, unless they are fiduciaries, their efforts are subject to other laws and are not covered by this act.").

64. CONN. GEN. STAT. § 45a-334a (2012); IDAHO CODE ANN. § 15-3-715(28) (2012); IND. CODE § 29-1-13-1.1 (2012); OKLA. STAT. tit. 58, § 269 (2012); R.I. GEN. LAWS § 33-27-3 (2012).

65. *See* Hopper, *supra* note 62.

66. Complaint at ¶¶ 4–6, Davis v. Google, Inc., No. 09CH15753 2009, 2009 WL 995128 (Ill. Cir. Apr. 9, 2009), *available at* http://www.courthousenews.com/2009/04/13/DavisvGoogle.pdf.

67. *Id.* at ¶ 10.

68. *Id.* at ¶ 7.

69. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT prefatory note (Proposed Discussion Draft Oct. 22, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013nov_FADA_Mtg_Draft.pdf.

cise that authority. In Part IV, this Note will discuss in detail what actions fall under the definition of "exercise control." Here, this Note will discuss the procedural and technical issues that surround the process of obtaining the authority to control digital property.

i. COURT ORDER REQUIREMENTS

Section Four of the FADAA Draft reads:

> (a) Unless prohibited by the will of the decedent, a court, or law of this state other than this [Act], a personal representative of the decedent may obtain:
>
> (1) the digital assets of a decedent;
>
> (2) records of the electronic communications of the decedent controlled by an electronic communication service or a remote computing service, including a log of the electronic address of each party with whom the decedent communicated; and
>
> (3) the contents of each electronic communication controlled by an electronic communication service or a remote computing service sent or received by the decedent, to the extent consistent with 18 U.S.C. Section 2702(b).

The FADAA Draft modeled this section after the Uniform Probate Code's definition of a personal representative's default powers.[70]

Whether fiduciary access to digital property should be a default power or whether it should require a court order to exercise such authority is still being debated by the Drafting Committee.[71] Making a personal representative's control over digital property a default power would be a huge shift in the disposition of digital property. If the FADAA Draft were to require court authorization and not be a default power the requirement may create some practical consequences, as not all wills go through a formal probate proceeding. Non-judicial officers, such as court clerks, appoint many personal representatives.[72] Some jurisdictions sign generic form letters of appointment for personal representatives.[73] The language in these forms will have to be changed to accommodate this requirement. Otherwise, families seeking to probate small estates will have to open more formal proceedings to get the authorization to dispose of digital property.

Personal representative authority over digital assets is limited by

---

70. *See* UNIF. PROBATE CODE §§ 3-715, 3-703 (amended 2010).

71. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 4 cmt. (Proposed Discussion Draft Jan. 18, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jan18_FADA_MtgDraft.pdf.

72. *Id.*

73. *See, e.g., Informal Probate: Application for Appointment as Personal Representative*, SUPERIOR CT. ARIZ. MARICOPA CNTY., *available at* http://www.superiorcourt.maricopa.gov/sscDocs/packets/pbip1f.pdf.

the clause that reads "[u]nless prohibited by the will of the decedent, a court, or law of this state other than this [act] . . . ."[74] This clause raises countless questions. What kinds of testamentary language will suffice to direct or limit the exercise of this control? What level of specificity is needed to restrict control? If the will is silent on the disposition of digital property, is a personal representative required to access or give the property to a residuary beneficiary? Will a new form of boilerplate that grants authority over all digital property without any specification as to specific accounts and assets suffice? Is a blanket rejection of authority over digital assets adequate? And if it is, what happens to this property?

If a testator provides in his will that the executor is to have no authority to access his digital assets, then the testator's estate will not be properly resolved. Testators cannot deny their executors authority to dispose of real property. Such a provision would cloud titles and create efficiency problems. The difference between many types of digital assets and real property is that some digital assets dispose of themselves over time. Many websites shut down accounts after periods of inactivity.[75] But other digital assets, such as money in online trading or savings accounts, will end up being abandoned if an executor cannot liquidate the accounts.

Imagine a simple will, where the testator leaves all of his stock and investments to his sister but specifically denies authority to his executor to access his digital accounts. If the testator had $5,000 worth of stock accessible through a traditional broker and $100,000 worth of stock kept in an E-Trade account, will the sister only inherit the $5,000? In such a scenario, litigation will likely ensue over the $100,000 worth of stock. Courts in cases such as this may override blanket rejections of authority. Otherwise, the real value of estates may be reduced and countless assets abandoned that would not normally be lost. At a minimum, this section of the FADAA Draft shows how critical it is for estate planners to work with their clients to create detailed and precise instructions for the distribution of digital assets. The provision also suggests that attorneys must specifically address the need for a court order with explicit authority over digital property.

---

74. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 4(a) (Proposed Discussion Draft Oct. 22, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013nov_FADA_Mtg_Draft.pdf.

75. *See, e.g.*, *Inactive Account Policy*, TWITTER, https://support.twitter.com/articles/15362-inactive-account-policy ("To keep your account active, be sure to log in and Tweet (i.e., post an update) within 6 months of your last update. Accounts may be permanently removed due to prolonged inactivity.") (last visited Dec. 29, 2013); *Terms of Service*, AOL, http://legal.aol.com/terms-of-service/full-terms/ (last updated Apr. 19, 2013) ("Your username and account may be terminated if you do not sign on a Service with your username at least once every 90 days.").

ii. Terms of Service

A personal representative can exercise control over a decedent's digital property in accordance with "any applicable and enforceable terms of service agreement."[76] This provision unfortunately requires us to look into every website's terms of service, terms of use, or privacy policy agreement to know what kinds of rights are available for a personal representative to control. Terms of service agreements that pop up on a website and require users to click "Agree" or "Continue" to access the website's content are called clickwrap or shrinkwrap agreements.[77] These agreements are generally upheld in court, so they will proscribe the testamentary options for digital assets.[78] If the clickwrap agreement includes terms creating a non-transferable license, as iTunes' does,[79] no asset is available to pass down. If the terms provide for user ownership of data, then subsequent terms must be analyzed to find the website's procedure for transfer of ownership.[80] If the website's terms of service do not address assignability and survivorship, then personal representatives will have to fight for access to that data on a case-by-case basis.[81]

The vast variations among these agreements in terms of assignability and ownership of online content reflect the various goals of Internet companies. Some companies limit transferability and assignability to protect the rights of their users,[82] while others limit user privacy and ownership rights in order to gather their users' information and content for advertising revenue purposes.[83] Facebook recently agreed to a $20-million settlement for marketing users' pictures and information to sell

---

76. Unif. Fiduciary Access to Digital Assets Act § 8(b).

77. Cheryl B. Preston & Eli W. McCann, *Unwrapping Shrinkwraps, Clickwraps, and Browsewraps: How the Law Went Wrong from Horse Traders to the Law of the Horse*, 26 BYU J. Pub. L. 1, 17–18 (2011).

78. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) ("Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general. . . ."). For an in-depth analysis of judicial enforcement of these agreements, see Preston & McCann, *supra* note 77.

79. *Terms and Conditions*, Apple, http://www.apple.com/legal/itunes/us/terms.html#SERVICE (last updated Sept. 18, 2013).

80. *See, e.g.*, *How Do I Close the PayPal Account of a Relative?*, PayPal, https://www.paypal.com/ca/webapps/helpcenter/article/?solutionId=1205004&m=SRE (last visited Oct. 20, 2013). PayPal requires executors to send it the decedent's death certificate and will or executor documentation. PayPal will issue a check in the account holder's name, if approved.

81. *See, e.g.*, *Terms of Service*, Yelp, http://www.yelp.com/static?country_=US&p=tos (last updated Nov. 27, 2012) (providing that users own their own content without including an assignability provision).

82. *See infra* text accompanying notes 86–91.

83. *Privacy Policy*, Google, http://www.google.com/policies/privacy/ (last modified Dec. 20, 2013) (providing that Google collects user information to "offer you tailored content—like giving you more relevant search results and ads").

its "Sponsored Stories" without user consent.[84] The settlement has limited how companies can use one's data in one respect, but it also shows how companies are getting increasingly creative in how they can limit user privacy and ownership in order to raise profits.

Internet users are becoming more acutely aware of their legal rights and what they are finding in their terms of service agreements. In December 2012, a public outcry erupted after Instagram announced a new terms of service and privacy policy that would have given advertisers free use of Instagram users' photographs without compensating the photographers.[85] Within days, Instagram backtracked and revised its policy changes.[86] Instagram's CEO posted a message on its site apologizing and affirming that "Instagram has no intention of selling your photos, and we never did. We don't own your photos—you do."[87] While this public relations nightmare made headlines, it highlights an instance of consumers actually *reading* and *responding* to what happens to their digital property.

Instagram's policy change outraged users for its encroachment on users' property rights, but other policies have been criticized for being too protective. For example, Yahoo! terminates all user rights upon the user's death.[88] When Yahoo! initially refused to release emails to the family of a fallen Marine, the public took notice.[89] Yahoo! argued that its policy was in place to protect its users' privacy.[90] Yahoo! eventually gave the family access, but it refused to change its policy.[91]

As more terms of service are litigated, restrictive policies may

84. Notice of Class Action and Proposed Settlement, Fraley v. Facebook, No. CV-11-01726 RS (N.D. Cal. Dec. 3, 2012), *available at* http:// docs.fraleyfacebooksettlement.com/docs/notice.pdf; *see also* Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, N.Y. TIMES, Nov. 30, 2011, at B1 (regarding a separate settlement between Facebook and the Federal Trade Commission due to unfair and deceptive use of user's personal information).

85. Jonathan Weber & Dan Levine, *Instagram Retreats on New Service Terms Following Backlash*, REUTERS (Dec. 21, 2012), *available at* http://www.reuters.com/article/2012/12/21/us-usa-instagram-changes-idUSBRE8BK03K20121221.

86. *Id.*

87. Kevin Systrom, *Updated Terms of Service Based on Your Feedback*, INSTAGRAM, http://blog.instagram.com/post/38421250999/updated-terms-of-service-based-on-your-feedback (last visited Dec. 29, 2013).

88. *Yahoo! Terms of Service*, YAHOO!, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last updated Mar. 16, 2012) ("You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death.").

89. Jim Hu, *Yahoo Denies Family Access to Dead Marine's E-mail*, CNET (Dec. 21, 2004, 2:49PM), http://news.cnet.com/Yahoo-denies-family-access-to-dead-marines-e-mail/2100-1038_3-5500057.html.

90. *Id.*

91. Stefanie Olsen, *Yahoo Releases E-mail of Deceased Marine*, CNET (Apr. 21, 2005, 12:39 PM), http://news.cnet.com/Yahoo-releases-e-mail-of-deceased-marine/2100-1038_3-5680025.html.

receive more scrutiny in the future. States enacting more uniform statutes that provide clear procedures for access to deceased users' accounts may allow online service providers to create more workable and user-friendly terms of service and privacy policies. But it will likely be public demand and responses like in the Instagram case that will force online service providers to better craft their terms to give more rights and disposition options to their users.

iii. Conservators, Agents, and Trustees

The FADAA Draft addresses digital property control by trustees, conservators, and agents under a power of attorney.[92] A trustee's authority is governed by the terms of the trust instrument.[93] The FADAA Draft trust provision needs to be expounded upon. Attorneys drafting trust instruments need guidance as to what language is needed to confer digital asset control in a trustee. They also need to know what limits can be put on that control. For example, there may be different requirements necessary to establish control of digital assets in testamentary and inter vivos trusts.

A conservator can obtain access to digital assets and electronic communications of a protected person after a hearing.[94] After they obtain access, conservators can "manage, deactivate, and delete" any of this information just as a personal representative of a decedent can.[95] A person acting under a power of attorney can also "access, manage, deactivate, and delete" digital information if the power of attorney documents grant the agent such authority.[96] This section was modeled after Uniform Probate Code § 5B-201(a), which outlines certain actions that require a specific grant of authority for a power of attorney to act.[97] Failure to gain express authority to handle digital assets could expose agents and conservators to liability under the SCA or other unauthorized

92. Unif. Fiduciary Access to Digital Assets Act §§ 5–7 (Proposed Discussion Draft Oct. 22, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013nov_FADA_Mtg_Draft.pdf.

93. *Id.* § 7 ("A trustee may access, manage, deactivate, and delete the digital assets and electronic communications held in the trust in accordance with the terms of the trust expressly authorizing the trustee to exercise these powers.").

94. *Id.* § 5.

95. *Id.* §§ 5(c)(4), 4(b). Section Six uses the same language as it relates to a "principal," rather than a "protected person."

96. *Id.* § 6.

97. Unif. Probate Code § 5B-201 reads as follows:

> (a) An agent under a power of attorney may do the following on behalf of the principal or with the principal's property only if the power of attorney expressly grants the agent the authority and exercise of the authority is not otherwise prohibited by another agreement or instrument to which the authority or property is subject . . . .

access laws.[98] Therefore, persons subjecting themselves or being subjected to conservatorships or power of attorney arrangements will need to explicitly outline what types of authority they wish to grant to an agent or conservator in the instruments governing those situations.

iv. Recovery from a Custodian

Recovering digital property from the custodian in possession of it is the next major hurdle for fiduciaries. Section Nine of the FADAA Draft provides a procedure for fiduciaries to recover digital property.[99] Fiduciaries must send a written request accompanied by certified copies of the applicable documentation granting that fiduciary control over the digital property.[100] The Act gives a custodian sixty days to comply, and a court order directing compliance can be requested after sixty days.[101]

Custodian compliance with written requests and court orders will determine the effectiveness of the Act. Section Ten of the FADAA Draft provides that a custodian acting in compliance with the Act is immune from liability.[102] Currently, online providers are not liable for disclosure violations of the SCA if done in good faith based on a court order,[103] but many service providers are still reluctant to turn over the information.[104] If the FADAA Draft or a similar law were widely enacted, custodians of electronic communications and property may be more assured that their release of property is lawful and may comply with written requests more consistently.

However, practical issues may arise with getting custodian compliance within sixty days. With certain sites having hundreds of millions of

98. *See* discussion *supra* Part III.A.

99. Unif. Fiduciary Access to Digital Assets Act § 9.

100. *Id.* § 9(b). If the fiduciary is a personal representative, a written request must be accompanied by a certified copy of the letter of appointment of the representative; if requested by a conservator, a certified copy of the court order giving the conservator authority of the digital property is needed; if requested by an agent, a certified copy of the power of attorney authorizing authority is needed; and if requested by a trustee, a certified copy of the trust instrument giving authority is required. *Id.*

101. *Id.* § 9(c).

102. *Id.* § 10.

103. 18 U.S.C. § 2703 (2012) reads as follows:

> (e) No cause of action against a provider disclosing information under this chapter.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

104. *See, e.g.*, *In Re* Request for Order Requiring Facebook, Inc. to Produce Documents and Things, No. C 12-80171 LHK (PSG), at *2 (N.D. Cal. Sept. 20, 2012), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/5:2012mc80171/257305/22/0.pdf?ts=1348220335.

users, custodians will likely need more support staff to handle all the requests. Companies may develop software that can process digital asset requests electronically, but new innovations entail development and implementation expenses. Staffing and logistical problems will likely be a barrier to getting companies to enact more favorable terms of service. Companies will want to eliminate the responsibility and expense of handling these requests.

IV. EXERCISING CONTROL

A. *Control*

After fiduciaries gain authority over digital property and systems are put in place for fiduciaries to retrieve the property from custodians, the last major question is: What kinds of actions are included under a fiduciary's ability to "access, manage, deactivate, and delete" digital property? The FADAA Draft needs a clear definition of these four terms in order to avoid unnecessary litigation. Fiduciaries will commonly request access to digital property to retrieve it and turn it over to a particular beneficiary or to delete said property. Whether certain types of assets can be devised or deleted should be spelled out in the statute. Complex distribution schemes such as devises with use restrictions will also need to be addressed in the statute. As new types of digital property are created, new creative ways of passing it on will inevitably appear. While the FADAA Draft cannot address all possible distribution schemes, limiting the number of case-by-case determinations on the enforceability of different testamentary provisions will increase the Act's success. Uniformity in how digital property is handled is key to getting custodians of digital property to release the property consistently and with less court involvement.

B. *Objections*

The January 2013 version of the FADAA Draft allowed interested parties to object to a fiduciary's control or continued control of a decedent's digital property.[105] However, the October 2013 version deleted this provision.[106] The ability of family members or interested parties to object should be protected. Many types of digital assets are extremely personal, and ownership of the assets may be unclear. It is helpful to

105. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 9 (Proposed Discussion Draft Jan. 18, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jan18_FADA_MtgDraft.pdf.

106. UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (Proposed Discussion Draft Oct. 22, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013nov_FADA_Mtg_Draft.pdf.

look for clues to the meaning of "access, manage, deactivate, and delete"[107] through the objections that interested parties may raise to challenge such control.

i. Assigning an Asset to a Particular Beneficiary

The first and most common bequest of digital property will likely be to give a specific digital asset to a particular beneficiary. Objections to outright gifts of digital property may resemble objections to a bequest of a family ring, such as improper execution, duress, or undue influence. These objections should apply to all digital assets in the same way, whether that asset is tangible, intangible, or metadata. Objections to outright gifts will likely not be objections to the digital or intangible nature of the asset, but rather objections to the beneficiary receiving it. Therefore, all digital assets should be devisable to a particular beneficiary (or group of beneficiaries, where feasible).

ii. Ordering Deletion of Digital Assets

Testators may order executors of their estates to delete a particular asset or all of their digital assets. It is easy to imagine a grieving family challenging such requests in court. Deletion of online data will likely be one of the most objected-to exercises of a fiduciary's control of a digital estate. Common law principles against waste and destruction of property do not exactly fit with digital asset concepts, yet they likely still apply in certain situations. Therefore, the FADAA Draft's definitions of "access, manage, deactivate, and delete" should specifically address what types of digital assets should be allowed to be deleted or whether the economic waste doctrine applies.

As discussed in Part I, different categories of digital assets serve different purposes and carry with them different monetary, cultural, and sentimental values. Therefore, it is important to apply the public policy against waste to each category separately. The first type of assets, access information, is a means to access other assets. These assets can very easily be taken to the grave if not written down or told to another person. This information can likely be equated to hiding the key to a safety deposit box or never writing down the combination to a safe. Therefore, a will provision ordering the deletion of a password or account number will likely not affect the testator's desired result. This situation would be like a testator ordering the destruction of the keys to his house, but this move will not stop someone from inheriting the house and changing the locks. Thus, practically speaking, access information should be allowed to be deleted, but such a move may not actually delete the information

107. Unif. Fiduciary Access to Digital Assets Act § 4(b).

within that account. Therefore, estate planners should not order account numbers and passwords to be deleted without ordering the assets that they guard to be deleted as well. Courts should allow interference with deletion of access information only if the testator willed property hidden behind that information to another. For example, a court may order an executor to use the access information to retrieve family pictures bequeathed to a beneficiary and then to delete the access information after the retrieval.

Testators should always be allowed to order metadata within their control to be deleted. Imagine a testator who exchanges emails with a mistress. He deletes the account and all record of the emails off of his computer. Yet, the deleted emails were backed up by the email provider and can be retrieved. The testator took all the steps he could during life to "destroy" this property, but the form of the website did not actually permanently destroy the property. This situation should be the equivalent of shredding torrid love letters, but instead it is the equivalent of keeping copies of the letters in the basement.

As discussed in Part I, most metadata and intangible digital assets should be deemed the property of the website or online business that hosts it. Therefore, a testator can only order deletion of that asset at death if the individual online host gives that power to the testator in its terms of service or other policies.

Tangible assets present the best case for applying the economic waste doctrine, but the doctrine should still be limited to assets of pure financial value or online businesses. Tangible digital assets such as pictures, music compositions, documents, and domain names can have great sentimental or monetary value. With so much business being conducted online, deleting data can lead to the loss of a revenue stream.

For many artists, computers are now the canvases, diaries, and sketch books of yore. Thus, a clear comparison can be made between artists wanting to destroy their unpublished creations and Internet users wanting to destroy their unpublished digital compositions and writings.[108] Historically, many of these assets kept in physical files and drawers have been barred from destruction. Yet, many artists and notable people have tried to order the destruction of their works at death. Lior Jacob Strahilevitz recounts that multiple American presidents have ordered destruction of their presidential papers after their deaths.[109] Franz Kafka ordered the executor of his estate to burn all of his writings.[110] In some of these cases, executors have refused to follow the

108. Lior Jacob Strahilevitz, *The Right to Destroy*, 114 YALE L.J. 781, 830 (2005).
109. *Id.* at 812.
110. *Id.* at 830–31.

testator's wishes on their own. In other situations, courts and Congress have stepped in to stop such destruction. In response to Nixon's destruction of papers relating to the Watergate scandal, Congress enacted the Presidential Records Act after Nixon's death that took away private ownership of presidential papers.[111]

Strahilevitz argues that we should defer to a testator's testamentary wishes when it comes to cultural property, even if that property also has a high monetary value.[112] His rationale is based on First Amendment issues and the rights of artists to define their own legacies and limit the release of "inferior works."[113] He further argues that if testamentary destruction is not allowed, destroying the property during life or willing the property to a company that will then destroy the property for the testator could circumvent the rule.[114] Strahilevitz's views demonstrate the balancing act that must be struck between privacy and freedom of testamentary disposition and waste of culturally and monetarily valuable property. Strahilevitz's views should be codified for personal digital property, even if the property has great cultural or financial value. Testators should have control over how they wish to leave their artistic legacy or, more simply, how they wish to leave their reputation among their family and friends.

Some digital assets are not personal compositions and take a purely financial or business form. Many blogs generate revenue from advertisements displayed on the site. If a testator directs his executor to delete the blog, the testator's heirs or other beneficiaries lose out on potential revenues. Destroying a blog can be seen as destroying the use of one's persona online, and such may be allowed under many states' right to publicity laws.[115] Right to publicity laws control the commercial use of a person's persona after his death.[116] Professor William A. Drennan, in discussing the ability of a celebrity to limit all commercial use of his persona after death, made the following analogy:

> [I]f a top celebrity enjoys the fruits of the commercial exploitation of her image until death, a direction in her will that her right of publicity can never be exploited would be comparable to allowing an individual to enjoy the interest and dividends from millions of dollars throughout her life, and then enforce a direction in her will to burn

111. *Id.* at 813.

112. *Id.* at 835.

113. *Id.* at 833.

114. *Id.* at 838.

115. William A. Drennan, *Wills, Trusts, Schadenfreude, and the Wild, Wacky Right of Publicity: Exploring the Enforceability of Dead-Hand Restrictions*, 58 ARK. L. REV. 43, 47, 141 (2005) (including compilation of state right to publicity laws).

116. *Id.* at 47.

the millions or hurl the millions into the sea.[117]

Drennan's argument parallels the problematic consequences of allowing testators to order the destruction of their financially profitable online businesses at death. They are in effect "hurling millions into the sea." Therefore, this author argues that testators cannot order the deletion of purely financial assets and online businesses earning revenue streams. Online savings accounts, online gambling accounts, and any other online accounts containing liquid assets should not be deleted without liquidating the cash value of the account and bequeathing it to a beneficiary first. The FADAA Draft should not allow an executor to delete blogs or websites with revenue streams at the testator's request if the court determines that the digital asset is the equivalent of a business. Distinguishing the line between personal digital property and a digital business may cause some court disputes in close cases, but including the distinction in the FADAA Draft will limit the number of deletion provisions that have to be decided on a case-by-case basis in clearer cases.

iii. Implementing Use Restrictions

As testators become more aware of their online assets and attorneys do more strategic estate planning with these assets, more creativity will arise in digital asset testamentary schemes. Creative testators may start to use other types of dispositions that less resemble fee simple dispositions and bequests and look more like life estate and conditional gift dispositions. For example, testators may put restrictions on the use of digital property into the future. The Uniform Law Commission Drafting Committee should decide what types of additional dead-hand controls can be applied to digital assets. The Committee must decide if the FADAA will limit which types of use restrictions can be put on digital assets or whether these decisions should be left for courts to decide on a case-by-case basis. While it is impossible for a statute to address all the possible ways that testators will try to devise their property, this author argues that the FADAA should address the major options in as much detail as possible and limit case-by-case determinations.

Use restrictions can take a variety of forms. Imagine a testator who owns a domain name. Can the testator will the domain name to X for life then to Y with the condition that the domain name be dormant during the life estate? The testator ostensibly interferes with the economic value of the domain name by ordering it to remain unused for years. The gift to X is valueless to X. Once Y's interest in the domain name becomes exercisable, he can benefit from the use or sale of the domain name. But

117. *Id.* at 94.

Y's benefit is delayed. Domain names may have very little cultural or sentimental value but have great monetary value. In 2001, the domain name "hotels.com" was purchased for roughly $11 million.[118] The president of hotels.com called the purchase "a bargain."[119] Thus, many digital assets have a value on the open market that varies greatly over time. Delaying the sale of a domain name (or any other digital asset) could mean losing hundreds to millions of dollars.

Another example of a problematic use restriction would be to will a blog to a beneficiary and then restrict the type of content that can be posted on the blog in the future. Professors Adam J. Hirsch and William K.S. Wang argue that use restrictions on traditional types of property lead to social costs, as they limit marketability and productive use of that property.[120] They argue that use restrictions also lead to private costs because "when a use restriction fails to correspond with the beneficiary's own consumption preferences, his utility falls."[121]

Courts have used a balancing test to determine what types of use restrictions will be enforced using the following factors: "(i) the nature of the property; (ii) the type of use restriction imposed; (iii) the testator's purpose in imposing the restriction; and (iv) the likely impact of the restriction on the heirs and society in general."[122] With the vast varieties of digital assets, employing this balancing test in the digital world is likely to lead to inconsistent holdings. Websites can disappear overnight or change their policies at any moment, which can make characterizing the nature of digital property difficult and the impact of the restriction on heirs and society unpredictable. Therefore, this author argues that use restrictions should be banned altogether for digital property. A judge should be able to override this rule in only the most exceptional circumstances.

CONCLUSION

Taking all of these concerns and consequences into consideration, testators should be able to require tangible digital assets to be bequeathed, in the online equivalent to fee simple, to any beneficiary or group of beneficiaries. Testators can also require that any tangible digital asset, except for an asset of pure financial value or an online business, be deleted or destroyed. Digital assets of pure financial value or

118. Interview by BBC Radio with David Roche, President, Hotels.com (Nov. 2, 2012), *available at* http://news.bbc.co.uk/today/hi/today/newsid_9765000/9765923.stm.

119. *Id.*

120. Adam J. Hirsch & William K.S. Wang, *A Qualitative Theory of the Dead Hand*, 68 IND. L.J. 1, 19–20 (1992).

121. *Id.*

122. Drennan, *supra* note 115, at 47.

online businesses, such as stock or cash in any online account, cannot be deleted because allowing otherwise would be a economic waste that is not a justifiable expression of testamentary freedom. This author suggests that the court's ability to override the deletion of any other digital property be very limited.

No assets should be allowed to be willed with life estates, use restrictions, or any other type of dead-hand restriction that interferes with one or more persons taking complete dominion over a particular asset. To allow otherwise would create enormous administrative problems for executors, beneficiaries, and online service providers. Complex ownership rights in digital property would be very difficult to enforce. Life estates or will provisions prohibiting deletion of digital property would add to the backlog of "digital junk" crowding the Internet. This rule could be amended at a later time if Web-service providers create clearer property rights in online content and systems for transferring ownership become easier to use. The current varieties of terms of service agreements and the reasons for their language suggest that clear user ownership is not desired or likely to occur.

Lastly, testators should be able to provide in their wills that their executor has no authority to access their digital property, but that such a provision can be overridden by court order. Complete bans of authority should be overridden only to avoid waste of purely financial assets and to handle disputes such as in the *Davis v. Google* case. Executors should be able to petition a court for access to an asset such as to avoid liability to an estate for libel or to liquidate cash kept online.

Certain digital property such as emails, websites, and domain names are well-established concepts that can be specifically provided for in the FADAA Draft. But the types of digital property owned on the Internet will continue to expand over the next twenty years, and certain concepts in the FADAA will need revision over time to include new types of digital property. Just because dictionaries will have to add new words in the future does not keep them from defining the words currently in existence.

Enforcing disposition choices with online service providers will be difficult. Issues will inevitably arise in deciding where to draw the line between destroyable and non-destroyable assets in close cases. Even with all these concerns, creating a Uniform Law with detailed provisions directing the disposition of digital property will move the conversation in the right direction. Having a well-drafted and thoughtful Uniform Law that states enact wholly or partially will be an authority for custodians to use to rethink their terms of service and better plan for the deaths of their users. A Uniform Law will give estate planners and testators much needed direction on how to lay their online selves to rest.