DEATH AND LIVE FEEDS:
PRIVACY PROTECTION IN FIDUCIARY ACCESS TO DIGITAL ASSETS

Jeehyeon (Jenny) Lee*

In 2014, the Uniform Law Commission approved the Uniform Fiduciary Access to Digital Assets Act (the "UFADAA") for enactment by states. The act gives fiduciaries broad access to digital assets, such as email and social media accounts, left behind by a decedent. Several states have already adopted laws regarding access to certain digital assets, but the UFADAA is distinctive in its asset-neutral approach, which treats digital assets like physical assets for the purposes of estate administration.

This Note argues that an asset-neutral approach to digital assets is fundamentally flawed, particularly with respect to social networking and social media content. Digital assets offer a level of comprehensiveness with regards to personal information that is unavailable from physical assets, both in nature and volume. Crucially, digital assets are also often linked to live, real-time feeds from other users' accounts, and thus provide access to others' digital assets.

The Note proposes changes to the UFADAA and the version of the act adopted by Delaware that recognize these differences between digital and physical assets. In order to protect the privacy of all users, both living and dead, the Note argues that fiduciary access should be limited to only the particular decedent's digital assets. Internet service providers should accordingly be required to restrict a fiduciary's access in this way and to exclude the digital assets of other living

* J.D. Candidate 2016, Columbia Law School; A.B. 2010, Harvard University. The author would like to thank Professor Michael A. Heller for his guidance and enthusiasm. She is grateful to her family for all their support, and to the editorial staff of the *Columbia Business Law Review* for their assistance in preparing this Note for publication.

users who are still connected to the decedent's accounts and assets.

I. INTRODUCTION

This Note explores an emerging issue at the intersection of estate administration and digital assets with the potential to significantly shift the way in which consumers, Internet

businesses, and the law deal with death and privacy: under the new model law proposed for adoption by states, decedents' fiduciaries are given unnecessarily broad access to the private information of decedents and third parties contained in digital assets, particularly social networking and media content. In July 2014, the Uniform Law Commission (the "ULC," also known as the National Conference of Commissioners on Uniform State Laws) approved the Uniform Fiduciary Access to Digital Assets Act ("UFADAA") and recommended it for enactment in all states.[1] The UFADAA seeks to provide general fiduciary access to digital assets by using the concept of media or asset neutrality; that is, if a fiduciary would have access to a tangible asset belonging to the decedent under existing law, that fiduciary will also have access to a similar type of digital asset, even if maintained by an internet service provider ("ISP").[2] The ULC's reasoning is that, for instance, since a fiduciary has the legal authority to inventory and dispose of all of a person's documents, "it should not matter whether those documents are printed on paper, stored on a personal computer, or stored in the cloud."[3] As such, the legally appointed fiduciary is empowered to "access, delete, preserve, and pass along digital assets as appropriate" under the UFADAA.[4]

1 *Uniform Fiduciary Access to Digital Assets Act*, UNIF. LAW COMM'N (2014), http://www.uniformlaws.org1/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2014_UFADAA_Final.pdf, *archived at* http://perma.cc/RBV9-B6Z8 [hereinafter UFADAA].

2 Press Release, Unif. Law Comm'n, Uniform Fiduciary Access to Digital Assets Act Approved (July 16, 2014), *available at* http://www.uniformlaws.org/NewsDetail.aspx?title=Uniform+Fiduciary+Access+to+Digital+Assets+Act+Approved, *archived at* http://perma.cc/SJA5-MFAS.

3 *Why Your State Should Adopt the Uniform Fiduciary Access to Digital Assets Act*, UNIF. LAW COMM'N, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/UFADAA%20-%20Why%20Your%20State%20Should%20Adopt%20-%20August%202014.pdf, *archived at* http://perma.cc/7XKV-ST2L (last visited Feb. 10, 2015).

4 *Id.*

Within a month of the UFADAA's approval, Delaware became the first state to adopt a version of the law when it passed House Bill No. 345, entitled the Fiduciary Access to Digital Assets and Digital Accounts Act (the "Delaware Act").[5] By the end of March of 2015, twenty-three other states had introduced bills based on the UFADAA.[6]

In comparison to existing state laws, the UFADAA and the Delaware Act are the most comprehensive to date in dealing with fiduciary access to digital assets, largely because of their asset-neutral approach.[7] Currently, only seven states have statutes governing any aspect of fiduciary authority over digital assets.[8] These state laws vary, however, with respect to the types of digital assets covered, the rights of the fiduciary, the category of fiduciary affected, and whether the principal's death or incapacity is covered.[9] For ISPs and their national and international users, these statutes are therefore unlikely to present a sustainable or comprehensive solution to an increasingly common issue.

This Note argues that the UFADAA and the Delaware Act, while recognizing a growing gap in estate administration, are nevertheless defective from a privacy standpoint because they make complete disclosure the default for fiduciaries. In particular, this Note proposes that the UFADAA and the Delaware Act should be amended to limit fiduciary access to only those digital assets that

5 Cyrus Farivar, *Delaware Becomes First State to Give Executors Broad Digital Assets Access*, ARS TECHNICA (Aug. 18, 2014, 4:15 PM), http://arstechnica.com/tech-policy/2014/08/delaware-becomes-first-state-to-give-heirs-broad-digital-assets-access, *archived at* http://perma.cc/CL24-LFDD.

6 *Legislation*, UNIF. LAW COMM'N, http://www.uniformlaws.org/Legislation.aspx?title=Fiduciary+Access+to+Digital+Assets (last visited Mar. 31, 2015), *archived at* http://perma.cc/5WGY-RMUW.

7 Farivar, *supra* note 5.

8 CONN. GEN. STAT. ANN. § 45a-334a (West 2014); IDAHO CODE ANN. §15-5-424(3)(z) (2014); IND. CODE ANN. § 29-1-13-1.1 (LexisNexis 2011); NEV. REV. STAT. ANN. § 143.188 (LexisNexis 2014); OKLA. STAT. ANN. tit. 58, § 269 (West 2014); R.I. GEN. LAWS § 33-27-3 (2011); VA. CODE ANN. § 64.2-110 (2012).

9 UFADAA, *supra* note 1, prefatory note.

belonged to the decedent and not other users, and to also provide for ISPs' responsibilities in enforcing those restrictions. The core of the current defects arises because neither the ULC nor Delaware law recognizes the distinctiveness of social media as an asset or addresses an asymmetry in the representation of privacy interests—the decedent has a fiduciary bound by fiduciary duties, but third parties who may have interests in the same digital asset are not separately required to be represented or protected by ISPs. Specifically, social media accounts offer a level of comprehensiveness with regard to personal information that is unavailable from physical assets, and are linked to live, real-time feeds from other users' accounts. This distinction is completely missed by the asset neutrality approach, when in fact, electronic communications are already protected in ways that tangible letters or messages are not through federal statutes like the Electronic Communications Privacy Act.[10] States may take different views regarding the relative power of fiduciaries and ISPs to determine access to decedents' accounts, and some may believe fiduciaries should have complete access as a default because ISPs currently wield too much control over the digital assets of users. This Note will conclude that, on balance, neither extreme is desirable, and proposes restrictions on both the fiduciaries and ISPs to protect third-party privacy, at least in the interim before courts can clarify several potential issues with the existing laws.

The ever-increasing importance of digital assets in consumers' lives (and post-mortem)[11] means that the issue of

10 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.)

11 *See* Robert Siciliano, *How Do Your Digital Assets Compare*?, MCAFEE BLOG CENTRAL (May 14, 2013), http://blogs.mcafee.com/consumer/digital-assets, *archived at* http://perma.cc/8GGB-4N9T. A McAfee survey released in May 2013 found that nearly 90% of consumers own multiple digital devices, and more than half of consumers spend 15 hours or more on their digital devices for personal use each week. More and more assets are being stored on devices, not to mention the cloud; on average, consumers globally have over $35,000 worth of assets stored on

fiduciary access to digital assets must be addressed soon by all states, and has the potential to significantly impact the relationship between ISPs and users. Part II of this Note surveys the definition of digital assets in the context of "digital death,"[12] with particular focus on social networking and media. It will discuss current tools available to users to express their post-mortem wishes, and the federal laws that may apply to these tools. Part III provides a snapshot of other state laws relating to fiduciary access to digital assets and an overview of the UFADAA, the Delaware Act, and the Privacy Expectation Afterlife and Choice Act. Part IV assesses the UFADAA and the Delaware Act against several articulated goals, and in doing so, details industry criticism and potential issues with the laws relating to privacy. Part V continues this discussion and calls for several changes to both the UFADAA and the Delaware Act that recognize critical differences between digital and physical assets.

II. BACKGROUND

A. Defining Digital Assets in Life and in Death

After a person dies, his or her personal representative—a fiduciary—is expected to fulfill three general functions: collecting and preserving the assets of the estate; paying creditors' claims, expenses of administration, and taxes; and distributing the remaining property to the decedent's devisees, legatees, or to intestate successors, as appropriate.[13] But as more of a person's life includes, and indeed, revolves around electronic transactions and

devices alone, including personal memories (such as photographs and videos), personal records (such as financial records and health information), and entertainment files. Interestingly, 55% of consumers surveyed said they stored digital assets that would be impossible to recreate, re-download, or re-purchase.

12 *See* Kristina Sherry, *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, 189 (2012).

13 ROBERT J. LYNN & GRAYSON M.P. MCCOUCH, INTRODUCTION TO ESTATE PLANNING IN A NUTSHELL 15 (6th ed. 2014).

interactions, digital assets can present complications to those trying to administer estates effectively.[14]

Since most probate codes and statutes do not mention digital assets, there is not yet a commonly accepted definition of digital assets.[15] There is, however, growing recognition amongst trust and estates experts that digital assets can contain "sentimental family heirlooms," such as photographs, as well as financial and personal records, and should at least be treated as "quasi-property" for the purposes of probate and trust administration.[16] Lawyers and industry experts have defined digital assets along several axes, such as location or purpose of the digital asset.[17] Broadly defined, digital assets are anything someone owns in a digital file stored either on a device or elsewhere via contract with the owner (including everything online, or in the cloud).[18]

Digital assets can be categorized in four ways: personal, social media, financial, and business.[19] Personal assets refer to those typically stored on a device or uploaded onto a website, and can include photographs, videos, and emails.[20] Social media assets, which this Note will focus on, "involve interactions with other people" on websites like Facebook or

14 Molly Wilkens, *Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?*, 62 HASTINGS L.J. 1037, 1041–42 (2011).

15 Suzanne B. Walsh, *Coming Soon to a Legislature Near You: Comprehensive State Law Governing Fiduciary Access to Digital Assets*, 8 CHARLESTON L. REV. 429, 431 (2014).

16 Nathan J. Dosch & Joseph W. Boucher, *E-Legacy: Estate Planning*, WISCONSIN LAWYER, Dec. 2010, at 11.

17 *See, e.g.*, Evan E. Carroll et al., *Helping Clients Reach Their Great Digital Beyond*, TRUSTS & ESTATES, Sept. 2011, at 66–68, http://wealthmanagement.com/estate-planning/helping-clients-reach-their-great-digital-beyond-0, *archived at* http://perma.cc/S8TY-9V3A (defining digital assets broadly by location and then examining different types of uses for digital assets).

18 *Id.*

19 Naomi Cahn, *Postmortem Life On-line*, 25 PROB. & PROP. 36, 36 (2011).

20 *Id.*

Twitter, as well as email accounts, and can be used for messaging and storage of assets, such as photographs.[21] For purposes of this Note, social media will be used to refer to both social networking accounts and social media—that is, an online account that allows the user to create and maintain relationships online.[22] Financial assets are financial accounts set up to be accessed via a computer, and may involve payment systems or accounts, such as PayPal.[23] Lastly, business accounts are those related to any type of commercial practice, such as customer orders and preferences, addresses, document storage, or domain names.[24]

A person's connections or networks were previously not considered assets that could be administered as part of an estate: "[e]ven an expanded view of an 'estate' does not include an element that is unquestionably valuable to those benefiting from it, namely, the network of personal, professional, political, and other connections created or cultivated by an individual that can open doors and enhance opportunities for favored family members . . . ."[25] But the number of people using social media has increased dramatically over the last few years—in February 2005, eight percent of Internet users utilized social networking sites, and by September 2013, the number had jumped to seventy-three percent.[26] As social networks become more

21 *Id.* at 37.

22 *Cf. Social Networking*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/social%20networking (last visited Feb. 10, 2015), *archived at* http://perma.cc/Z24C-WBX7 (defining "social networking" as "the creation and maintenance of personal and business relationships especially online").

23 Cahn, *supra* note 19, at 37.

24 *Id.*

25 Lynn & McCouch, *supra* note 13, at 12.

26 *Social Networking Fact Sheet*, PEW RESEARCH CTR., http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet (last visited Feb. 10, 2015), *archived at* http://perma.cc/9FE9-LHQ5. According to the Pew Research Center, as of September 2014, 23% of online adults used Twitter, 71% used Facebook, 26% used Instagram, 28% used Pinterest, and 28% used LinkedIn. Notably, as of August 2012, 46% of

common and well-established, then, this notion that a decedent's "connections" cannot be considered part of his or her estate may soon undergo a change.

Social media accounts in particular are different from personal, financial, and business accounts because their value comes specifically from being linked to other accounts, sometimes across multiple platforms, and do not have a tangible equivalent. Being connected on social media essentially means to have access to the digital assets of others. This can include someone else's personal information, photographs, videos, posts, and "likes." Indeed, a person's social media use can be described as a "presence,"[27] which attests to both the personal nature of social media accounts as well as the difficulty of fitting social media into a traditional property type.

As new technology develops, the definition and types of digital assets will undoubtedly expand,[28] and it is not difficult to identify multiple reasons why people may want to engage in digital asset planning to enable their fiduciaries to access their digital assets after they die. Digital access for a fiduciary could help prevent identity theft and allow the fiduciary to successfully manage non-digital assets that are tied to digital accounts.[29] Fiduciaries can also properly identify assets that have actual or sentimental value, and honor the decedent's wishes regarding who should or should

adult Internet users posted original photos or videos online that they themselves created.

27 *See, e.g.,* Stephanie Sammons, *A 7-Step Process for Expanding Your Online Media Presence*, SOCIALMEDIATODAY (Sept. 18, 2013), http://www.socialmediatoday.com/content/7-step-process-expanding-your-online-presence, *archived at* http://perma.cc/HHH7-2ASF.

28 *See, e.g.*, Nermin Hajdarbegovic, *What Will Become of Your Bitcoins When You Die?*, COINDESK (Apr. 16, 2014), http://www.coindesk.com/will-become-bitcoins-die, *archived at* http://perma.cc/H4MF-WWJL. There is uncertainty surrounding how bitcoins, a form of digital currency, should or could be distributed after death. Bitcoin use can be pseudo-anonymous, with layers of encryption and authentication.

29 Gerry W. Beyer & Naomi Cahn, *When You Pass On, Don't Leave the Passwords Behind: Planning for Digital Assets*, 26 PROB. & PROP. 40, 41 (2012).

not have access to the assets.[30] Within the current legal framework, policies can vary from state to state and from one ISP to another, so having a record of the decedent's express wishes may provide some direction in navigating these laws and contracts.[31]

B. Current Options and Barriers to Fiduciary Access to Digital Assets

Several options are available to users if they want to distribute their digital assets after death. A few ISPs offer users a choice; Google, for instance, offers an Inactive Account Manager feature that enables users to determine how they want their accounts and data to be handled if their accounts are inactive for a set period of time.[32] Users can set their data to be deleted after three, six, nine or twelve months of inactivity, or designate selected contacts to receive data.[33] More generally, estate attorneys and experts offer insights online on how to manage digital assets,[34] and digital estate planning (DEP) services can be used to create online accounts where individuals list or store their digital assets and indicate what should happen to them following their deaths.[35] For example, PasswordBox's Legacy Locker service

30 *Id*. at 41–42.

31 *Id*. at 41.

32 Andreas Tuerk, *Plan Your Digital Afterlife with Inactive Account Manager*, GOOGLE (Apr. 11, 2013), http://googlepublicpolicy.blogspot.com/2013/04/plan-your-digital-afterlife-with.html, *archived at* http://perma.cc/5W8Q-YWU9.

33 *Id*. It is unclear, however, what percentage of Google users proactively make use of this service or even know of its existence.

34 *See, e.g.*, THE DIGITAL BEYOND, http://www.thedigitalbeyond.com (last visited Apr. 20, 2015), *archived at* http://perma.cc/2HKV-L3NP; *see also* Beyer & Cahn, *supra* note 29. Professors Beyer and Cahn suggest supplementing one's will with a separate document containing login information, as probated wills become public record. The document should lay out how each asset is to be handled, including which should be deleted and which should be kept and by whom.

35 *See, e.g.*, AFTERNOTE, http://www.afternote.com (last visited Apr. 20, 2015), *archived at* http://perma.cc/H5MW-6J3V. For a list of services, *see Digital Death and Afterlife Online Services List*, THE DIGITAL BEYOND,

allows users to store, retrieve and share passwords, and upon presentation of a death certificate, will pass on the information to the user's designated "digital heir."[36] There are questions, however, surrounding the legality of these DEP services and whether they are the most reliable way to transfer digital assets.[37]

Despite these options, fiduciaries face several barriers to entry. First, the decedent and the ISP likely enjoyed a contractual relationship. If the decedent agreed to terms of service ("TOS") when signing up for a service, the agreement may prohibit access to a third party.[38] For instance, Facebook's TOS provides that "[y]ou will not share your password . . . let anyone else access your account, or do anything else that might jeopardize the security of your account."[39] Facebook reserves the right to stop providing all or part of its services to a user if he or she "violate[s] the letter or spirit of this Statement, or otherwise create[s] risk or possible legal exposure for [Facebook] . . . ."[40] Even if the decedent had voluntarily given her fiduciary the login information to her Facebook account, this would theoretically be in violation of the TOS and could give Facebook the right to terminate its services and deny access to whatever digital assets were in the account.[41]

Second, an individual who accesses another individual's online account without the account holder's authorization or consent may be subject to civil or criminal penalties under

http://www.thedigitalbeyond.com/online-services-list (last visited Apr. 20, 2015), *archived at* http://perma.cc/D7GR-DBHH.

36 LEGACY LOCKER, http://www.passwordbox.com/legacylocker (last visited Apr. 20, 2015), *archived at* http://perma.cc/V85Y-95SJ.

37 James D. Lamm, Christina L. Kunz, Damien A. Riehl & Peter John Rademacher, *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries From Managing Digital Property*, 68 UNIV. OF MIAMI L. REV. 385, 406–11 (2014).

38 *Id*. at 388.

39 *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/legal/terms (last updated Feb. 17, 2015), *archived at* http://perma.cc/8MY4-WDH8.

40 *Id*.

41 Lamm et al., *supra* note 37, at 399.

federal and state privacy laws.[42] Certain federal and state laws, such as the Computer Fraud and Abuse Act ("CFAA"), prohibit unauthorized access of computer hardware and devices and their stored data.[43] ISPs also face potential liability under the Stored Communications Act ("SCA"), contained in Title II of the Electronic Communications Privacy Act of 1986 ("ECPA").[44] Under the SCA, providers of public communications services are prohibited from disclosing the contents of users' communications unless one of the specified exemptions applies.[45] Notably, if someone has the "lawful consent" of "the originator or an addressee or intended recipient of such communication[s], or the subscriber," then the provider may voluntarily disclose electronic communications to a third party.[46] Social media account contents will most likely be deemed "communications" under the SCA,[47] but there has not yet been definitive judicial resolution of the relevant preemption issues.

Ultimately, a sustainable and comprehensive solution to the issue of fiduciary access to digital assets should take into account the interests of ISPs, digital asset holders, and fiduciaries of decedents. This Note proposes prioritizing the following four goals, adapted from an earlier articulation[48]: (1) respecting privacy and observing federal and state laws relating to privacy; (2) honoring decedents' post-mortem wishes; (3) efficient disposal of digital assets and execution of fiduciary duties; and (4) minimizing probate, litigation, and

42 Walsh, *supra* note 15, at 432–33.

43 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, 18 U.S.C. § 1030 (2012). *See* Suzanne Brown Walsh & Conrad Teitell, *Protecting Clients' Digital Assets*, TRUSTS & ESTATES, 33 (2014).

44 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 18 U.S.C. §§ 2510-2522, 2701-2712 (2012).

45 18 U.S.C. § 2702(b).

46 *Id.* § 2702(b)(3).

47 Walsh & Teitell, *supra* note 43, at 34. *See* Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1260 (2012).

48 *See* Sherry, *supra* note 12, at 190.

other administrative "hassles." These goals recognize the interests of the main stakeholders—account holder, fiduciary, ISP, and other users. This Note will look to each of these goals in turn, with its focus on privacy, in assessing the UFADAA and Delaware Act.

III. LAWS RELATING TO FIDUCIARY ACCESS TO DIGITAL ASSETS

A. Existing State Laws

Seven states—Connecticut, Idaho, Indiana, Oklahoma, Rhode Island, Nevada, and Virginia—currently have statutes related to fiduciary access to digital assets.[49] The statutes cover executors or administrators of estates, court-appointed guardians or conservators of estates, agents appointed under powers of attorney, and trustees in varying degrees. While the evolution of these state laws reflects growing understanding of both the need for fiduciaries to access digital assets and the diversity of digital assets themselves, one shortcoming that several share is that they are specific to the kinds of technologies available at the time they were enacted.[50] Another criticism is that these laws do not address the issue of TOS between ISPs and users, and by using varying language, such as "access or copies" in the Connecticut and Rhode Island laws, they leave open the question of who has the power to make the determination of what kind of access fiduciaries get.[51] Finally, the issue of preemption still remains since there has been no ruling on whether these state laws are preempted by the CFAA or SCA. The varied nature of even these seven state laws demonstrates the utility of a unified approach, especially because of the possibility of federal preemption and the fact

49 CONN. GEN. STAT. § 45a-334a (2013); IDAHO CODE ANN. §15-5-424(3)(z) (2011); IND. CODE § 29-1-13-1.1 (2013); NEV. REV. STAT. § 143.188, OKLA. STAT. tit. 58, § 269 (2013); R.I. GEN. LAWS § 33-27-3 (2011); VA. CODE. ANN. § 64.2-110 (2012).

50 Gerry W. Beyer & Naomi Cahn, *Digital Planning: The Future of Elder Law*, 9 NAELA J. 135, 147 (2013).

51 *Id.*

that many ISPs serve users across the country. In comparison to these state laws, the UFADAA is a more comprehensive response to the issue of fiduciary access to digital assets.

B. Uniform Law Commission: The Uniform Fiduciary Access to Digital Assets Act

In light of the growing need for fiduciaries to deal with digital assets, and the several barriers that they face in doing so, the ULC set out to ensure that legally appointed fiduciaries could access, delete, preserve, and pass along digital assets as appropriate.[52] The purpose of the UFADAA is to remove barriers to a fiduciary's access to electronic records, while respecting the privacy and intent of the account holder.[53] As such, under section 8, the fiduciary, "subject to the terms-of-service agreement, copyright law, and other applicable law, may take any action concerning the asset to the extent of the account holder's authority and the fiduciary's power under the law of this state other than this [act] . . . ."[54] The UFADAA's limits are delineated by its definition of "digital assets," which applies only to electronic records.[55] A "record" in turn is defined as information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.[56]

The UFADAA applies to four types of fiduciaries who are granted access to digital assets: (1) personal representatives of a decedent's estate (section 4); (2) guardians or conservators of a protected person's estate (section 5); (3)

52 Press Release, Unif. Law Comm'n, *supra* note 2.

53 UFADAA, *supra* note 1, at Prefatory Note, 1–2.

54 *Id.* at § 8(a).

55 *Id.* at § 2(9).

56 *Id.* at § 2(21). The comments to UFADAA clarify that records can include information stored on devices, content uploaded onto website, and rights in digital property such as domain names. *See id.* at § 2 cmt.

agents under a power of attorney (section 6); and (4) trustees (section 7).[57]

The UFADAA appears to govern only *access* to digital assets, while deferring to other law to determine ownership or disposition of the assets.[58] In section 9, however, the UFADAA allows fiduciaries to request access to *and* control of the asset from custodians—the comments to the section clarify that "control" means the ability to move (unless prohibited by copyright law) or delete that particular asset.[59] Access is granted to the fiduciary for the limited purpose of carrying out his or her fiduciary duties[60] and is subject to

---

57 *Id. at* Prefatory Note; *see Fiduciary Access to Digital Assets Act Proposed Discussion Draft* (Feb. 7, 2013), UFADAA § 9 http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013feb7_FADA_MtgDraft_Styled.pdf, *archived at* http://perma.cc/3FD3-KRAP. The February 2013 draft of the UFADAA allowed an interested party to object in court to a fiduciary's request for control over or the fiduciary's exercise of continued control over digital property; *see also id.* at § 9 cmt, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013feb7_FADA_MtgDraft_Styled.pdf, *archived at* http://perma.cc/3FD3-KRAP. The accompanying commentary contemplates the issue of waste: "The Committee may want to provide guidance on when a court might preclude access . . . under what circumstances, based, for example, on public policy against burning Rembrandts, could the court override the will?" *Id.* This recognition of the rights of "interested parties," however, is omitted in the final version, UFADAA, *supra* note 1, and only the rights of the four types of fiduciaries are provided for.

58 Memorandum from Suzanne Brown Walsh, Chair, Unif. Law Comm'n, to Comm. of the Whole, 2014 ULC Annual Meeting, Seattle on Uniform Fiduciary Access to Digital Assets Act, Final Reading (May 27, 2014) at 2, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2014am_ufadaa_issues%20memo.pdf, *archived at* http://perma.cc/MB9R-ZBLV.

59 UFADAA, *supra* note 1, § 9(a)(1)–(2) states: "[I]f a fiduciary with a right under this [act] to access a digital asset of an account holder complies with subsection (b), the custodian shall comply with the fiduciary's request in a record for: (1) access to the asset; (2) control of the asset . . . ."

60 *The Uniform Fiduciary Access to Digital Assets Act – A Summary*, UNIF. LAW. COMM'N, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/UFADAA%20-%20Summary%20-%20August%202014.pdf (last visited Apr. 20, 2015), *archived at* http://perma.cc/EK5D-DG6V. The summary gives one example: "Thus, for

TOS agreements and copyright or other applicable law.[61] The UFADAA thus operates under the traditional trusts and estates legal framework.[62]

Section 8 attempts to confront the CFAA and SCA head-on. The fiduciary is deemed to have, under applicable electronic privacy laws, the "lawful consent" of the account holder for the custodian to divulge electronic communication content to the fiduciary, and also to be an "authorized user" under applicable computer fraud and unauthorized access laws.[63] These terms correspond with those in sections 2701 and 2702 of the SCA, and section 1030 of the CFAA respectively.[64] Section 8 further provides that if a provision

example, an executor may access a decedent's email account in order to make an inventory of estate assets and ultimately to close the account in an orderly manner, but may not make public the decedent's confidential communications or impersonate the decent by sending email from the account." *Id.*

61 UFADAA, *supra* note 1, § 8(a)(1).

62 UFADAA, *supra* note 1, Prefatory Note. Specifically, under § 3-711 of the Uniform Probate Code (UPC), the executor "has the same power over the title to property of the estate that an absolute owner would have, in trust however, for the benefit of the creditors and others interested in the estate. This power may be exercised without notice, hearing, or order of court." § 3-703 of the UPC provides that the executor "is under a duty to settle and distribute the estate of the decedent in accordance with the terms of any probated and effective will and this Code, and as expeditiously and efficiently as is consistent with the best interests of the estate."

63 UFADAA, *supra* note 1, § 8(a)(2)–(3).

64 Section 2701(a) of the SCA levies criminal penalties upon anyone who "(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. . . ." 18 U.S.C § 2701(a)(1)–(2). Section 1030 of the CFAA, also using the language of authorization, provides penalties for anyone who "intentionally accesses a computer without authorization or exceeds authorized access." *Id.* § 1030(a). Section 2702 of the SCA prohibits certain ISPs that provide an electronic communication service to the public from disclosing the contents of digital account. *Id.* § 2702(b)(3). Providers can voluntarily disclose electronic communications content to a third party only if an exception applies, including the "lawful consent" of the originator, an addressee or intended recipient, or the subscriber. *Id.* § 2702(b)(3).

in a TOS limits a fiduciary's access to digital assets, the provision is void against the strong public policy of whichever state has adopted the act, unless the account holder has agreed to a provision by "an affirmative act" separate from the other provisions of the TOS.[65] A choice-of-law provision in a TOS agreement is also unenforceable against a fiduciary to the extent the provision designates a law that limits the fiduciary's access.[66]

Section 9 details compliance and provides that a custodian shall comply with a fiduciary's request to access, control, and obtain copies of assets (to the extent permitted by copyright law)[67] within 60 days after receipt.[68] "Control" means only the ability to move or delete; for example, if the account holder has a computer game character and in-game property associated with an online game, then the fiduciary's ability to sell the character or the in-game property, is controlled by traditional probate law.[69] Thus, access and control are to be construed within the boundaries of "enabling the fiduciary to do electronically what the account holder could have done electronically."[70]

Section 10 of the UFADAA grants immunity to custodians for an act or omission done in good faith in compliance with the act.[71] While custodians may be subject to direct liability for noncompliance with a judicial order issued under section 8 of the act, indirect liability arising from granting a right of access under the act is subject to immunity.[72] The ULC's commentary notes that access to a digital asset may invade the privacy or harm the reputation of the decedent or the family of the decedent, but the custodian would be immune

65 UFADAA, *supra* note 1, § 8(b).

66 *Id.* at § 8(c).

67 *Id.* at § 9(a)(1)–(3).

68 *Id.* at § 9(c).

69 *Id.* at § 9 cmt.

70 *Id.*

71 *Id.* at § 10.

72 *Id.* § 10 cmt.

from liability arising out of these circumstances if it had acted in good faith to comply with the act.[73]

C. Delaware: Fiduciary Access to Digital Assets and Digital Accounts Act

Delaware is the first and only state to adopt a version of the UFADAA thus far, and the law came into effect in January of 2015.[74] The Delaware Act, titled Fiduciary Access to Digital Assets and Digital Accounts, defines "digital assets" more broadly than the UFADAA. It includes electronic records, similar to the UFADAA, such as data, text, emails, documents, video, and social media content.[75] It also includes, however, computer source codes, computer programs, software, software licenses, and databases,[76] which may be protected by intellectual property. In addition, the Delaware Act covers "digital accounts," which refers to electronic systems for information that provides access to a digital asset—email accounts, social network accounts, and domain service accounts, among others.[77]

Section 5004 is titled "Control of digital accounts and digital assets by a fiduciary," which appears at first to be a departure from the access-oriented language of the UFADAA. The Delaware Act provides that "a fiduciary may exercise control over any and all rights in digital assets and digital accounts of an account holder, to the extent permitted under applicable state or federal law, including copyright

---

73 *Id.*

74 *See* Legislative Fact Sheet – Fiduciary Access to Digital Assets, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets (last visited Apr. 20, 2015), *archived at* http://perma.cc/4VLL-9QRP. Delaware is the only state that has enacted the UFADAA so far, but at least 13 states have introduced bills for 2015 relating to fiduciary access to digital assets, including Florida, Indiana, Kentucky, Nebraska, New Mexico, North Dakota, Virginia, and Washington.

75 12 DEL. C. § 5002(7).

76 *Id.*

77 *Id.* § 5002(6).

law, or regulations or any end user license agreement."[78] Section 5005(b), however, gives the fiduciary ability to request "access to, transfer of, copy of, or destruction of a digital asset or digital account," which is substantially similar to the ability to move or delete assets given under the UFADAA. Fiduciaries are defined to include personal representatives, guardians, agents, trustees, and advisors, the last category being an addition to those of the UFADAA.[79]

The Delaware Act tracks the UFADAA for most of its substance and structure. The Delaware Act similarly provides that any provision in an end user license agreement that limits a fiduciary's access or control over a digital asset or account of an account holder is void as against the strong public policy of the state, unless the account holder agreed to such a provision by an affirmative act separate from his or her asset to other provisions of the end user license agreement.[80] Choice-of-law provisions are dealt with as under the UFADAA.[81] In addition, a fiduciary has the same access as the account holder and is deemed to (i) have the lawful consent of the account holder, and (ii) be an authorized agent or user under all applicable state and federal law and regulations and any end user license agreement.[82] Custodians are given 60 days after receipt of a valid written request for access to comply under the law, as proposed in the UFADAA.[83] Finally, a custodian acting in good faith in compliance with the chapter is immune from liability.[84]

In other sections, the Delaware Act expands upon or adds to the suggested provisions from the UFADAA. Section 5005(b) states that the custodian must comply with a fiduciary's request unless it would be "technologically

78 *Id.* § 5004(a).

79 *Id.* § 5002(11).

80 *Id.* § 5004(b).

81 *Id.* § 5004(c).

82 *Id.* § 5005(a).

83 *Id.* § 5005(d).

84 *Id.* § 5006(g).

impracticable" to do so.[85] The Delaware makes specific reference to the ECPA in this section and provides that the fiduciary may access the content of an electronic communication, as defined in the ECPA, only if the custodian is permitted to disclose the content under the ECPA.[86]

In terms of compliance, the Delaware Act also varies from the UFADAA in that it holds a custodian immune from civil liability if, acting in good faith, it accidentally destroys any digital asset or account subject to the chapter.[87] Perhaps most significantly, a custodian who refuses to accept a valid written request in violation of the act faces a court order and also liability for damages, including reasonable attorney's fees and costs.[88] In contrast, the UFADAA only provides for court orders as a remedy.[89]

D. Corporate and Civil Liberties Organizations: Privacy Expectation Afterlife and Choices Act

In response to the UFADAA, NetChoice, a trade association of e-commerce and online businesses including Facebook, Inc., Google Inc., Yahoo!, Inc., eBay Inc., and AOL Inc., put forth its own version of an act providing for more limited access to fiduciaries.[90] The Privacy Expectation Afterlife and Choices Act ("PEAC") stands in stark contrast to the UFADAA and the Delaware Act in several important aspects. First, PEAC requires an executor or administrator seeking access to an account to obtain an order from a court of probate. Second, PEAC provides for separate access to

85 *Id.* § 5005(b).

86 *Id.* § 5005(b)(1).

87 *Id.* § 5006(g).

88 *Id.* § 5006(e)(1)-(2).

89 UFADAA, *supra* note 1, § 9(c).

90 *Privacy Expectation Afterlife and Choices Act (PEAC)*, NETCHOICE, http://netchoice.org/library/privacy-expectation-afterlife-choices-act-peac (last visited Apr. 20, 2015), *archived at* http://perma.cc/7JEJ-RVGL [hereinafter PEAC].

records of accounts,[91] specifically in order to resolve fiscal assets, and to contents of records, which are only obtainable with the express consent of the deceased user. Third, in granting access to records, the court must make findings of facts confirming that, *inter alia*, access does not violate applicable laws, the request is narrowly tailored to effect the purpose of the administration of the estate, the executor or administrator demonstrates a good faith belief that the records are relevant to resolve fiscal assets, the request does not seek information beyond a year prior to the date of death, and the request is not in conflict with the decedent's will or testament.[92] If a court grants access to contents, it must first find that the decedent "expressly consented" either through a will or setting within the product or service—PEAC thus recognizes user settings to be equivalent to a will or testament in this respect—and also indemnify the provider "from all liability in complying with the order."[93] Fourth, PEAC states that the court should quash or modify an order if compliance would cause an "undue burden" on the ISP.[94] Fifth, with no exceptions, the ISP "cannot be required to allow any requesting party to assume control" of the account.[95]

PEAC is supported by both corporate and civil liberties organizations, which have voiced numerous criticisms of the UFADAA approach. NetChoice emphasizes the difference between physical and digital assets—for example, electronic communications are stored by default, require several steps to delete, are more akin to voice communications than

91 PEAC thus defines records differently from the UFADAA. The UFADAA refers to electronic information as records; PEAC, on the other hand, refers to information "like the To and From lines of an email" as records. *See Privacy Afterlife: Empowering Users to Control Who Can See Their Online Accounts*, NETCHOICE, http://netchoice.org/library/decedent-information (last visited Apr. 20, 2015), *archived at* http://perma.cc/W9NA-QR6F.

92 PEAC § 1(A).

93 *Id.* § 1(B).

94 *Id.* § 2.

95 *Id.* § 5.

letters, and involve a third-party custodian that is subject to federal privacy laws.[96] It argues that the ULC approach only considers the fiduciary's interests, disregarding the privacy interests of third parties and decedents, and puts businesses at odds in complying with federal or state law.[97] A joint letter from the Center for Democracy & Technology and other civil liberties organizations, such as the American Civil Liberties Union ("ACLU"), also points to critical differences between kinds of assets, adding that there is a wide array of types of digital assets—including dating profiles, health and fitness data, and voicemail—which may have varying consumer expectations attached to them.[98] The letter separately notes that conservatorships should not be included in digital estates legislation, as they are in the UFADAA, because conservatorships are meant to assist protected living, not deceased, persons.[99]

This Note will focus on assessing the UFADAA and Delaware Act given the growing number of states introducing bills based on the UFADAA, but it is nevertheless instructive to examine the gulf between the PEAC and UFADAA approaches. The differences suggest that several major ISPs anticipate significant impact on their businesses as a result of broad and standardized fiduciary access to digital assets. Indeed, in simple terms, the UFADAA gives broad access to electronic information to four types of fiduciaries, subject to relevant laws, while granting immunity to ISPs for good faith compliance with the act. It overrides certain TOS provisions, gives control over accounts to fiduciaries, and does not require the express consent of the decedent or the approval of a probate court.

These UFADAA provisions carry huge potential changes to the types and nature of services offered by ISPs, the degree of control ISPs have over digital assets, and the

96 *See Privacy Afterlife*, *supra* note 91.

97 *Id.*

98 Letter from Ctr. for Democracy & Tech., et al. (Jan. 12, 2015), http://cdt.org/files/2015/01/Joint-Letter-re-ULC-Bill-general-statement-2-FINAL.pdf, *archived at* http://perma.cc/45MD-27Y3.

99 *Id.*

extent of liability they face in dealing with fiduciary requests and user privacy. First, ISPs may have to change the structure, nature, or policies of their products and services to clarify which digital assets a user would want shared after death. As will be discussed in Part IV, several ISPs like Google have already created tools to help users define which parts of their accounts are to be shared. Since the UFADAA recognizes a user's affirmative act separate from the decedent's assent to other parts of the TOS, more ISPs may implement this kind of explicit structure to their products and TOS. Overall, this could be a very positive development; even the Center for Democracy & Technology suggests that "lawmakers should consider which of these models (or another alternative) would create an incentive structure that encourages companies to develop and nudge users to express their wishes proactively."[100] On the other hand, as more people seek broad access to decedents' accounts, ISPs will need to ascertain the wishes of living users who are connected to those decedents and modify accordingly the nature of relationships between users. Again, while these may be practical changes that should happen over time anyway, it will require ISPs to implement a level of customization and monitoring that is likely not essential to users' day-to-day interactions with their products and services.

ISPs also stand to lose a considerable amount of control over digital accounts and assets. Where most ISPs currently have exclusive control over the TOS governing a user's account and activities, the UFADAA nullifies certain provisions that maintain an ISP's exclusive control over who accesses accounts and how those accounts are accessed following death. For certain sensitive or personal data, it is possible that an ISP may decide it is worthwhile to stop acting as custodian altogether. For example, various applications (also referred to as "apps") and attachments

100 Alethea Lange, *Everybody Dies: What is Your Digital Legacy?*, CTR. FOR DEMOCRACY & TECH. BLOG (Jan. 23, 2015), http://cdt.org/blog/everybody-dies-what-is-your-digital-legacy, *archived at* http://perma.cc/HWZ6-TQU6.

have been developed for the smartphone to allow individuals to monitor their health and even make diagnoses. Apps to monitor one's mental health and to analyze photographs of skin conditions have already been developed, and smartphone attachments will soon allow individuals to perform an array of routine lab tests.[101] If an ISP maintains data from such an app in the cloud or elsewhere, a fiduciary could theoretically gain access to it, perhaps without even intending to. To avoid complications arising from scenarios of this type, the ISP may decide not to store the data, which would then limit the product's capabilities and user choices, or implement a more complex TOS structure that allows the user to make explicit his or her wishes. Moreover, ISPs have an interest in ensuring that accounts are not used in an inappropriate manner after the user's death; "trolling" of inactive accounts can cause emotional distress to families of decedents, and ISPs have raised concerns that allowing fiduciary access may hinder their efforts to detect and stop such activity.[102] Critically, ISPs could lose consumer confidence because of this reduction in control, particularly if people feel that individuals they are not "friends" with could gain access to their profiles without their approval.

The greatest complications for ISPs, however, will likely arise from potential legal liability as a result of the UFADAA and fiduciary access to others' accounts. Because the UFADAA does not require fiduciaries to go through a court first, the ISP will need to engage in some level of legal analysis to process individual requests, which may be time-consuming and expensive. Of course, the UFADAA grants immunity to ISPs that comply in good faith with its requirements[103] but, as pointed out in the joint letter from civil liberties organizations, this does not resolve questions of

101 Eric J. Topol, *The Future of Medicine Is in Your SmartPhone*, WALL ST. J.: LIFE (Jan. 9, 2015, 1:37 PM), http://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

102 *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, 439–40 (2014).

103 UFADAA, *supra* note 1, § 10.

federal law. For one, the ECPA exception allowing providers to voluntarily disclose contents of communication requires consent of the author or his or her agent. But it is not clear whether executors or other court-appointed personal representatives are legally agents or have the lawful consent of the deceased subscriber under federal law, even if the UFADAA claims to grant this under state law.[104] Should the ISP decide to grant access, it will then have to determine how much access to provide in responding to a request. This could require the ISP to assess the decedent's account and its contents first, if it decided against providing blanket access to the whole account. If dealing with an email account, would the "To," "From," date, and subject fields suffice to allow the fiduciary to execute his or her duties? With a social media account, could the ISP withhold any chat records and still be held to be acting in good faith? The ISP might find itself also having to delineate the very boundaries of digital assets—if a decedent is tagged in photographs that are uploaded by another user, should the fiduciary have access to those? The UFADAA immunizes the ISP in instances where third parties may claim invasion of privacy or harm of reputation,[105] but ISPs will still need to somehow ensure user satisfaction and comfort over the long term and across its overall user base. Given the clearly competing control and privacy stakes of the issue, this Note proposes using the four goals mentioned above in order to account for the interests of various parties before proposing modifications to the UFADAA.

IV. ASSESSING THE UFADAA AND THE DELAWARE ACT

This section assesses the acts against the articulated four goals, focusing primarily on privacy. The next section suggests that the laws should limit fiduciary access to only those digital assets belonging to decedents and their

104 *See* Letter from Ctr. for Democracy & Tech., *supra* note 98.

105 UFADAA, *supra* note 1, § 10 cmt.

accounts, and impose an affirmative obligation on ISPs to grant fiduciaries this limited access to the extent possible.

A. Respecting Privacy and Observing Federal and State Laws Relating to Privacy

The first articulated goal of fiduciary access to digital assets—respecting and observing privacy interests and laws—is the most hotly contested issue between the laws' proponents and industry parties. Yahoo, for one, posted a statement titled, "Your Digital Will: Your Choice," on its blog on September 15, 2014, expressing concern that the ULC's legislation does "not ensure the privacy of sensitive or confidential information shared by the decedent or third parties . . . [and] is based on the faulty presumption that the decedent would have wanted the trustee to have access to his or her communications."[106] Yahoo was one of several companies and industry groups, including Google and the State Privacy & Security Coalition, to sign a veto request letter (hereinafter Industry Veto Letter) to Governor Jack Markell of Delaware in July 2014.[107] The letter argued that the bill "removes privacy protections for Delaware citizens, overrides user privacy choices, sets the privacy of Delaware residents lower than the federal standard, [and] forces businesses to choose between violating a state law and risking violating a federal one . . . ."[108]

Popular social media or email websites[109] utilize a wide range of policies for how accounts and digital assets are

106 Bill Ashworth, *Your Digital Will: Your Choice*, YAHOO! GLOBAL PUBLIC POLICY (Sept. 15, 2014), http://yahoopolicy.tumblr.com/post/97570901633/your-digital-will-your-choice, *archived at* http://perma.cc/UUX2-NFSX.

107 Letter from AOL, et al., to Jack Markell, Governor, Del. (July 8, 2014), http://netchoice.org/wp-content/uploads/Industry-Veto-Request-of-DE-HB-345-Signed.pdf, *archived at* http://perma.cc/VY8B-3PNH [hereinafter *Industry Veto Letter*].

108 *Id.*

109 *See generally* Marcelo Ballve, *Our List of the World's Largest Social Networks Shows How Video, Messages, and China Are Taking Over the Social Web*, BUS. INSIDER (Dec. 17, 2013), http://www.business

disposed of following an account holder's death, which will be surveyed below. In attempting to provide a unified procedure, the UFADAA and the Delaware Act are problematic for two main reasons: they may be preempted by federal laws and they conflict with evolving notions of privacy in the digital world. This section will survey current industry standards, privacy laws, and notions of privacy in assessing the acts.

1. Current Industry Standards

When signing up for a social media, email, or other online service, users typically agree to TOS set by the ISP—this is the case with companies such as Google, Facebook, Twitter, Yahoo! Mail, and Instagram. While most users neither read nor understand these TOS, courts have usually deemed users to have read and accepted the terms in adhesion-style contracts.[110]

Yahoo represents one end of the spectrum by adhering to a policy where they honor the initial TOS with the decedent and prohibit the transferring of accounts or information contained therein: "Yahoo cannot provide passwords or access to deceased users' accounts, including account content such as email."[111] People are able to make requests to have a decedent's account closed, to suspend services, and to have "any contents permanently deleted for privacy."[112]

Significantly, these TOS give ISPs technical control over accounts, which has led to conflicts between contractual rights and the rights of beneficiaries and families. An oft-

insider.com/the-worlds-largest-social-networks-2013-12, *archived at* http://perma.cc/J2FZ-KBM3 (discussing the popularity of various social networks and other sites).

110 *See* Lilian Edwards & Edina Harbinja, *What Happens to My Facebook Profile When I Die?: Legal Issues Around Transmission of Digital Assets on Death* 3 (Feb. 21, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2222163, *archived at* http://perma.cc/U67L-XDXG.

111 *Options Available When a Yahoo Account Owner Passes Away*, YAHOO! HELP, http://help.yahoo.com/kb/SLN9112.html (last visited Apr. 20, 2015), *archived at* https://perma.cc/JR9F-RS2X.

112 *Id.*

cited case is that of Justin Ellsworth, a U.S. Marine who was killed in action in Iraq in 2004, and his family who sought access to Justin's Yahoo email account following his death.[113] Yahoo denied the request, citing the TOS to which Justin had agreed when he opened his account.[114] Justin's family litigated the issue and, in 2005, the Probate Court of Oakland County, Michigan ordered Yahoo to give the contents of Justin's emails to his family.[115] The judge allowed Yahoo to abide by its TOS by not compelling Yahoo to divulge login information, and instead, ordering Yahoo to provide the contents of the account in a CD.[116] It is important to note here, however, that the Ellsworth family's efforts to access Justin's emails may not be considered part of the usual probate-related purposes of disposing of digital assets—it appears that they wanted to access his emails for sentimental purposes, which are not sufficient alone to gain access to digital assets under UFADAA or the Delaware Act.[117] If the Ellsworth family had been seeking access for a typical probate-related purpose, such as winding up financial accounts, the acts may have allowed them to bypass the court process altogether, minimized their interactions with Yahoo, and made clearer the expectations on both parties.

113 *See* Dosch & Boucher, *supra* note 16, at 11–12.

114 Edwards & Harbinja, *supra* note 110, at 7.

115 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, *archived at* http://perma.cc/9PA2-JP9B.

116 Edwards & Harbinja, *supra* note 110, at 7.

117 Sentimental objects are sometimes dealt with outside of the typical estate planning process. In referring to digital assets, one practice guide noted that "the digital asset would appear to be more akin to a family heirloom or sentimental object than a valuable tangible asset that would require a post-mortem administration." Frederick K. Hoops, Frederick H. Hoops III & Daniel S. Hoops, *Digital Assets*, 2 FAMILY ESTATE PLANNING GUIDE § 34:19 (4th ed.) (database updated Oct. 2014). Another guide recommended encouraging clients to dispose of items of intrinsic value in wills and to use separate writing to pass on property with more sentimental value. Linda R. Getzen & Edward F. Koren, *Gifts of Tangible Personal Property—Separate Writings*, 2 EST. TAX & PERS. FIN. PLAN. § 18:23 (Dec. 2014).

Towards the other end of the spectrum of access, Google offers an Inactive Account Manager that allows users to delete or permit access to their account after a certain period of inactivity.[118] By contrast, Facebook "memorializes" the accounts of deceased users, which means the account is effectively locked.[119] No one can log into or modify the account, but Friends are still able to share memories on the decedent's Timeline and send private messages to the decedent.[120] Friends or family can request memorialization of an account.[121] For the digital assets themselves, Facebook's policies allow users to designate others as "legacy contacts" to "look after" memorialized accounts.[122] To deactivate an account, Facebook requires a "special request" from an immediate family member or executor.[123]

In more minimalist fashion, other ISPs provide procedures for simply deactivating accounts upon proper notification of a user's death, which allow them greater control over the process of deactivating and managing accounts of deceased users. Twitter will deactivate an account upon receipt of certain documentation, but states that "[we] are unable to provide account access to anyone regardless of his or her relationship to the deceased."[124]

118 *Inactive Account Manager*, GOOGLE, http://www.google.com/settings/account/inactive (last visited Apr. 20, 2015), *archived at* https://perma.cc/HB4J-Z9HR.

119 *Memorialized Accounts*, FACEBOOK, http://www.facebook.com/help/1506822589577997 (last visited Apr. 20, 2015), *archived at* http://perma.cc/A9FN-BRQS.

120 *Id*.

121 *Memorialization Request*, FACEBOOK, http://www.facebook.com/help/contact/651319028315841 (last visited Apr. 20, 2015), *archived at* http://perma.cc/MC3U-XMQT.

122 *What Is a Legacy Contact?*, FACEBOOK, http://www.facebook.com/help/1568013990080948 (last visited Apr. 20, 2015), *archived at* https://perma.cc/7GJ5-W2SG.

123 *Special Request for Deceased Person's Account*, FACEBOOK, http://www.facebook.com/help/contact/228813257197480 (last visited Apr. 20, 2015), *archived at* https://perma.cc/Y44Y-CPZV.

124 *Contacting Twitter About a Deceased User or Media Concerning a Deceased Family Member*, TWITTER HELP CENTER, http://support.twitter.com/articles/87894-contacting-twitter-about-a-deceased-user-or-

Twitter does allow immediate family members and other authorized individuals to request the removal of images or video of deceased individuals. It reserves the right, however, to consider "public interest factors such as the newsworthiness of the content" and notes that it "may not be able to honor every request."[125] Instagram similarly makes no promises, but encourages individuals to contact it in the event of a user's death.[126]

2. Electronic Privacy and Fraud Laws

Commentators have noted that federal privacy laws could preempt laws that give fiduciaries access to electronic communications and information,[127] while others have reached the opposite conclusion.[128] Notably, neither the SCA

media-concerning-a-deceased-family-member# (last visited Mar. 3, 2015), *archived at* http://perma.cc/5HDT-3ECD.

125 *Id*.

126 *Privacy Policy*, INSTAGRAM, http://instagram.com/about/legal/privacy/# (last visited Apr. 20, 2015), *archived at* http://perma.cc/D2PR-4G4S.

127 *See, e.g.*, William Bissett & David Kauffman, *Understanding Proposed Legislation for Digital Assets*, J. FIN. PLAN., Apr. 2014, at 16, 18 (explaining that ISPs must currently abide by existing federal law to protect the privacy rights and interests of users).

128 *See* Jim Lamm, *Thoughts on the Stored Communications Act, Federal Preemption and Supremacy, and State Laws on Fiduciary Access to Digital Property*, DIGITAL PASSING BLOG (Nov. 4, 2013), http://www.digitalpassing.com/2013/11/04/thoughts-stored-communications-act-federal-preemption-supremacy-state-laws-fiduciary-access-digital-property, *archived at* http://perma.cc/V9MN-FQEC (concluding that the UFADAA as of its November 2013 draft is not in conflict with and is not preempted by the SCA); *see also* William Bissett & David Kauffman, *Surf the Evolving Web of Laws Affecting Digital Assets*, EST. PLAN., Apr. 2014, at 32, 35 (stating that because the fiduciary is given the same authority as the deceased account holder, the fiduciary is "authorized" by the deceased account holder as required under the CFAA and SCA); Naomi Cahn, *Probate Law Meets the Digital Age: Harmonizing Federal Law With State Wealth Transfer Law on Digital Assets*, 67 VAND. L. REV. 1697, 1725 (2014). Naomi Cahn argues that even if the SCA did apply, the UFADAA is not preempted:

nor the CFAA mentions fiduciaries. Suzanne Walsh, Chair of the UFADAA Drafting Committee, maintains that the UFADAA satisfies these privacy concerns by recognizing the account holder's ability to prevent fiduciary access to a digital asset, as they would be able to with traditional assets under existing law.[129] While a separate analysis of the preemption issue is beyond the scope of this Note, this section will provide a survey of the applicable federal laws and how courts have interpreted the laws in the context of digital assets to date.

The Industry Veto Letter sent to the Governor of Delaware argued that the Delaware Act forces businesses to choose between violating a state law and risking violating a federal one, citing the ECPA.[130] One set of external comments to the May 2013 version of the UFADAA draft questioned whether a court would find a state law controlling, given the applicable federal legal issues. Specifically, the comments note that giving access to a fiduciary of a decedent who dies intestate—and as such, has not been given explicit consent to access the decedent's digital assets—does not satisfy the ECPA.[131] The final version of the UFADAA, however, does not distinguish between decedents who die intestate and those who had wills at death.

> [A]lthough the state has no power to compel an ISP to take an action that is contrary to federal law, where federal law permits the action and a state then compels it, the two laws can be interpreted as in harmony. That is, ISPs can comply with state-law mandates without violating the SCA.

Id.

129 Walsh, *supra* note 58.

130 Industry Veto Letter, *supra* note 107.

131 Letter from Steve DelBianco, Exec. Dir., NetChoice, Carl M. Szabo, Policy Counsel, NetChoice & James J. Halpert, Gen. Counsel, State Privacy & Sec. Coal., to Suzanne Brown Walsh, Unif. Law Comm'n (July 8, 2013), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jul_FADA_NetChoice_Szabo%20et%20al_Comments.pdf, *archived at* http://perma.cc/GH9R-6FF3.

Though the CFAA and the SCA were enacted in the 1980s, long before the rise of social media, they may still apply in full force to digital assets and accounts today. The CFAA of 1984 provides criminal sanctions[132] against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[133] The United States Court of Appeals for the Ninth Circuit has interpreted "authorization" to mean any permission at all.[134] The CFAA may also cover computers and servers that support service providers.[135] In addition, all fifty states criminalize unauthorized access to computers, systems, or networks,[136] usually requiring as elements (1) access to a computer, system, or network; (2) with knowledge; and (3) without authorization or in excess of authority, though many states fail to define "authorization."[137]

The SCA prohibits public providers of electronic communication services[138] ("ECS") from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service . . . ."[139] The act also prohibits public providers of remote computing services[140] ("RCS") from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that

132 18 U.S.C. § 1030(c) (2012); *see* Lamm et al., *supra* note 37, at 400.

133 18 U.S.C. § 1030(a)(2)(C).

134 *See, e.g.*, LVRC Holdings v. Brekka, 581 F.3d 1127, 1132–33 (9th Cir. 2009) (defining "authorization" as any permission at all).

135 *See* Lamm et al., *supra* note 37, at 400.

136 *Id.* at 402; *see, e.g.*, ARIZ. REV. STAT. ANN. § 13-2316(A)(8) (2013); MASS. ANN. LAWS ch. 266, § 120F (LexisNexis 2010).

137 Lamm et al., *supra* note 37, at 402.

138 Electronic communication service is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications . . . ." 18 U.S.C. § 2510(15).

139 *Id.* § 2702(a)(1).

140 Remote computing service means "the provision to the public of computer storage or processing services by means of an electronic communications system . . . ." *Id.* § 2711(2).

service . . . ."[141] The SCA only applies to public providers of ECS or RCS, so employers or school email services are excluded.

There have been several cases where courts have deemed certain social media-related communications to be subject to the SCA, including private messages and Twitter.[142] Because social media ISPs are either involved in the active and current transmission of electronic communications or provide storage space for users, nearly every social media ISP is covered under the SCA.[143] The Ninth Circuit has held that email messages stored on a server are protected under the SCA,[144] while the United States District Court for the Southern District of New York has held that privacy settings for YouTube videos determine the SCA's applicability to them—videos saved as private were protected under the SCA, but public videos later removed were not.[145]

In contrast to the Ninth Circuit, the Massachusetts Court of Appeals has left open the question of whether Yahoo should disclose emails to estate administrators. In a 2013 case, Yahoo denied a co-administrator authority to access the content of his deceased brother's emails.[146] The surviving brother had originally set up and shared access to the account but had since forgotten the password.[147] Yahoo moved to dismiss the declaratory action based partly on the California forum designation provision in its TOS, reasoning that the emails were not property of the estate.[148] The court

141 18 U.S.C. § 2702(a)(2) (2012).

142 *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) (ruling that private messages sent through web-based email provider or through social networking are subject to the SCA); People v. Harris, 945 N.Y.S.2d 505, 511 (Crim. Ct. 2012) (holding Twitter to be an electronic communication provider under the SCA).

143 Borden, *supra* note 102, at 416.

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

145 Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264–65 (S.D.N.Y. 2008).

146 Ajemian v. Yahoo!, Inc., 987 N.E.2d 604, 608–09 (Mass. App. Ct. 2013).

147 *Id.* at 608.

148 *Id.* at 609–10.

concluded that it was not reasonable to enforce the forum selection and limitations clauses against the administrators of the estate, in part because they were not parties to the TOS.[149] The appeals court remanded to the probate court the ultimate questions of whether the contents of the email account are property of the estate and whether SCA barred Yahoo from disclosing the contents of the email account to the administrators.[150]

The relevant exception under the SCA allows for the right to disclose information "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of [RCS]."[151] Lawful consent, however, is not defined by the statute, and in a Facebook discovery case, the court held that the SCA prevents an ISP from disclosing stored communications in response to civil subpoenas. In the case, Sahar Daftary, a model, had died after falling from her boyfriend's apartment building in Manchester, England.[152] Her family members subpoenaed Facebook in California to find information in her account that could be used to show Daftary's state of mind at the time of death as part of the coroner's inquest to determine whether her death was a suicide or suspicious.[153] Facebook objected to the subpoena, and argued that it was unclear whether an executor could provide "lawful consent" to Facebook for the purpose of disclosing information from the decedent's account.[154] Alternatively, Facebook asked the court to hold that the fiduciary had lawful consent and to compel Facebook to disclose the content at issue.[155]

The court did not rule on whether the fiduciary could provide lawful consent and quashed the subpoena,[156] but did

149 *Id.* at 613–14.

150 *Id.* at 615–16.

151 18 U.S.C. § 2702(b)(3) (2012).

152 *In re* Facebook, Inc., 923 F. Supp. 2d 1204, 1205 (N.D. Cal. 2012).

153 *Id*.

154 Motion to Quash Subpoena in a Civil Case at 6–7, *In re* Facebook, Inc., 923 F. Supp. 2d 1204 (N.D. Cal. Aug. 6, 2012) (No. 5:12-mc-80171).

155 *In re* Facebook, 923 F. Supp. 2d at 1205.

156 *Id.* at 1206.

acknowledge that "nothing prevents Facebook from concluding on its own that Applicants have standing to consent on [the decedent's] behalf and providing the requested materials voluntarily."[157] Indeed, the SCA does not compel an ISP to disclose private account records; rather, it authorizes voluntary disclosure, so even if the court was persuaded that the applicants' consent on Daftary's behalf satisfied the SCA requirements, a subpoena *compelling* production had to be quashed.[158] The court noted, "[t]o rule otherwise would run afoul of the 'specific [privacy] interests that the [SCA] seeks to protect.'"[159]

While courts have not ruled on whether the SCA or CFAA applies to fiduciaries, commentators are undoubtedly divided. One commentator points to judicial interpretations of "authorization" under the CFAA as "power granted by authority,"[160] and argues that this should cover a fiduciary named in a will or trust, or even authorized by a probate court order. For the "lawful consent" language of the SCA's section 2702, some view consent and authorization as related, but others note that while authorization under section 2701 can be given by a probate court, consent under section 2702 must stem from the user.[161]

157 *Id*.

158 *See* 18 U.S.C. § 2702(b)–(c) (2012) ("A provider . . . may divulge the contents of a communication [if an exception applies].").

159 *In re* Facebook, 923 F. Supp. 2d at 1206 (alteration in original) (quoting Theofel v. Farey-Jones, 359 F.3d 1066, 1074 (9th Cir 2004)). The court referenced *United States v. Rodgers*, 461 U.S. 677, 706 (1983), and its reasoning that "[t]he word 'may,' when used in a statute, usually implies some degree of discretion," in understanding the phrase "may divulge the contents" in the SCA. *See id.* at 1206 n.7.

160 David Horton, *The Stored Communications Act and Digital Assets*, 67 VAND. L. REV. 1729, 1731 (2014) (quoting LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)).

161 *Id*. at 1734–35.

3. Evolving Digital Assets, Evolving Notions of Privacy

In the context of digital assets, privacy is of particular concern to account holders because many digital accounts are linked to those of others—and typically are voluminous and more personal in nature than physical assets. These aspects of digital assets should be taken into account when giving fiduciaries access.

Privacy rights are generally deemed to cease upon death.[162] As such, under traditional probate and trust law, private letters, diaries, and photographs can be inherited. Several commentators have examined the third-party privacy argument with respect to email accounts, which may contain confidential and highly sensitive emails from patients or clients,[163] and dismissed this concern as nothing new since physical correspondence and files may contain sensitive information as well.[164] But this line of argument takes a narrow view of digital assets, and does not account for different digital capabilities available to users, including the various ways and far greater number of people one can communicate with electronically.

Digital assets are fundamentally different from physical assets, to such a degree that treating them as the same would result in inequities and privacy violations. The idea that some digital assets cannot be equated or analogized to physical assets, and therefore, require separate treatment, was raised to the ULC during the drafting process. In a letter to the ULC dated July 3, 2013, the ACLU highlighted a fundamental difference between digital and physical assets and underlined privacy concerns for individuals whose information is shared and individuals with whom the account holder communicated online:

---

162 *See* RESTATEMENT (SECOND) OF TORTS § 652I (1977). There are exceptions for the appropriation of one's name or likeness.

163 Farivar, *supra* note 5.

164 Jonathan J. Darrow & Gerald R. Ferrara, *Who Owns a Decedent's Emails: Inheritable Probate Assets or Property of the Network?,* 10 N.Y.U. J. LEGIS. & PUB. POL'Y, 281, 313 (2007).

> In many ways, digital estates differ not just in degree, but in kind, from their offline analogues. This is to say that individuals do not simply retain more correspondence in online storage than they ever could in paper form, but that the keys to an individual's online accounts are likely to provide access to highly sensitive materials, such as internet dating profiles, that lack offline equivalents. In short, new technologies may require new approaches to old problems, including the settling of estates.[165]

Lee Rowland, a Staff Attorney with the ACLU's Speech, Privacy and Technology Project, similarly believes that real-time access to a user's account and its functions (such as search and chat) is never proper for a fiduciary because it represents a living thread, one in which other individuals might have expectations.[166]

The idea that digital information is different in both degree and kind proved foundational to the Supreme Court case *Riley v. California*, where the Court held that police cannot search digital information on an arrested individual's cell phone without a warrant.[167] Chief Justice Roberts reasoned that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[168] These "privacies" may not even have physical equivalents because "[a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."[169]

---

165 Letter from Allison S. Bohm, Advocacy & Policy Strategist, ACLU, to Suzanne Brown Walsh, Chair, & Professor Naomi Cahn, Reporter, Unif. Law Comm'n (July 3, 2013) (on file with author), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jul3_FADA_Comments_ACLU.pdf, *archived at* http://perma.cc/JU5G-ZCND.

166 Telephone Interview with Lee Rowland, Staff Attorney, ACLU (Nov. 12, 2014).

167 Riley v. California, 134 S. Ct. 2473, 2493 (2014).

168 *Id.* at 2494–95 (internal citations omitted).

169 *Id.* at 2491.

Moreover, cloud computing may extend the breadth of information available through the cell phone.[170] Justice Alito agreed on this point in his concurrence: "Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form."[171]

The asset-neutrality approach of the UFADAA and the Delaware Act completely overlooks these important distinctions of volume and nature between digital and physical assets. The frequency with which people use their digital accounts and assets may help account for how voluminous and personal this information is—sixty-four percent of Facebook users visit the site on a daily basis,[172] ninety-four percent of teen social media users have a Facebook profile,[173] and teens share increasingly more information about themselves on social media sites, including photographs, interests, relationship statuses, and videos.[174] As of August 2013, adult Facebook users had an average of 338 Friends.[175]

Furthermore, certain digital assets track parts of a user's life that are typically not recorded in the physical world, adding to the differences in volume and nature of digital assets. Location tracking through a global positioning system (GPS) may be collected as data in a person's cell phone or via a tool in a person's social media account. For example, Facebook and Instagram allow users to "check in" to places

170 *Id.*

171 *Id*. at 2496 (Alito, J., concurring).

172 Aaron Smith, *6 New Facts about Facebook*, PEW RESEARCH CENTER (Feb. 3, 2014), http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook, *archived at* http://perma.cc/6ZFM-PQV7.

173 Mary Madden, *Teens Haven't Abandoned Facebook (Yet)*, PEW RESEARCH INTERNET PROJECT (Aug. 15, 2013), http://www.pewinternet.org/2013/08/15/teens-havent-abandoned-facebook-yet, *archived at* http://perma.cc/UD2X-9TTC.

174 Mardy Madden et al., *Teens, Social Media, and Privacy,* PEW RESEARCH INTERNET PROJECT (May 21, 2013), http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy, *archived at* http://perma.cc/7ZXM-2QF5.

175 Smith, *supra* note 172.

when creating posts. This kind of record about a person's day-to-day whereabouts over a period of time is not something that is usually available as a physical record for fiduciaries. Another example is records from a chat function attached to an email, social media, or gaming account. These chats are closer to conversations in the physical world than correspondence; they happen in real time with another person. As a result, these digital assets offer a comprehensiveness of information about a person's life that is normally unavailable in the physical world. That comprehensiveness itself could change in the near future—it is estimated that by 2015, more Americans will access the Internet via mobile devices than desktop computers[176] so there could be further shifts in the kind of data collected about an individual.

Another fundamental flaw of the asset-neutrality approach is that it ignores the live nature of some digital assets; that is, granting fiduciaries access to certain digital assets and accounts will automatically give them *live* access to the assets and accounts of third parties. In fact, the two most disliked aspects of Facebook, as reported by the Pew Research Center, are "people sharing too much information about themselves" and "others posting things about you or pictures of you without asking permission."[177] In third place was "other people seeing posts or comments you didn't mean for them to see."[178] These disliked features of Facebook attest to the intensely personal nature of social media content the abundance of personal information about users, and the fact that content related to a user is not necessarily generated only by the user. Most critically, they point to the interactive nature of social media and that all Facebook users are

176 *Digital Government*, THE WHITE HOUSE, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html (last visited Apr. 20, 2015), *archived at* http://perma.cc/NGJ3-QVDQ.

177 Aaron Smith, *6 New Facts about Facebook*, PEW RESEARCH CENTER (Feb. 3, 2014), http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook, *archived at* http://perma.cc/6ZFM-PQV7.

178 *Id*.

connected to other users—the very point of having an account is to have others see your profile and to be able to view other profiles. In the context of fiduciary obligations mentioned above, ongoing and live access to other users' accounts through the decedents' account is unnecessary. If the fiduciary needs to collect names and contact details of friends and acquaintances to alert them of the account holder's passing, this can be done with information or records contained within the account without contact or access to others' accounts.

By adopting an asset-neutral approach, the UFADAA and Delaware Act are severely limited in their ability to take into account evolving notions of digital privacy, which has proved central to both consumers and ISPs. At the industry level, online privacy is clearly a recognized concern: ISPs have been held accountable by the Federal Trade Commission ("FTC") for deceiving customers in relation to privacy promises. In 2011, for example, Facebook settled with the FTC after Facebook violated certain promises and policies, including statements that when users deactivated or deleted their accounts, their photographs and videos would be inaccessible, and that users could restrict sharing of data to limited audiences.[179] The settlement required Facebook to ensure it lived up to its promises in the future by giving consumers "clear and prominent notice and obtaining consumers' express consent before their information is shared beyond the privacy settings they have established."[180] In light of the volume and nature of digital assets, and the already clear recognition of privacy as an issue related to these digital assets, the UFADAA and the state laws based on it should provide for stronger privacy protections.

179 Press Release, Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, (Nov. 29, 2011), http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep, *archived at* http://perma.cc/3RPF-X642.

180 *Id*.

B. Honoring Decedents' Post-Mortem Wishes; Efficient Disposal of Digital Assets and Execution of Fiduciary Duties; and Minimizing Probate, Litigation, and Other Administrative Hassles

In addition to privacy concerns, the laws also raise issues in relation to the three other articulated goals. First, in order to honor account holders' post-mortem wishes, it must be clear what those wishes are. If the account holder's wishes are that they do not want the fiduciary to access any or certain digital assets, the UFADAA and the Delaware Act do not mention ways to recognize this other than in a will or TOS agreed to by an affirmative act separate from the account holder's assent to other provisions. Many people die intestate,[181] and since the ISPs are not under any obligation to ask users to affirmatively make a choice about post-mortem access to their accounts, the acts may risk failing to capture a critical part of the decedents' wishes. Even those who leave wills behind may neglect to consider digital assets as part of their estate.

For efficient disposal of digital assets and execution of fiduciary duties, it is crucial that the laws make clear how fiduciaries can gain access and ensure that access is not impeded unnecessarily. The UFADAA and Delaware Act both provide substantively for access to and control of assets in general—the ULC law primarily uses "access" to mean the ability to move and delete assets, whereas the Delaware Act uses "control" to mean access to, transfer of, copying of, or destruction of assets. Neither the UFADAA nor the Delaware Act, however, makes clear whether ISPs are expected to transfer login details to fiduciaries or just copies of contents. An ISP, for instance, could give discretionary access to content and prohibit transfer of account login details, but it is unclear whether that satisfies the good faith

181 For instance, some estimates claim that around half of Americans with children die without a will. *See, e.g.*, Lisa Scherzer, *Half of Americans With Kids Set to Die Without a Will*, YAHOO! FINANCE (May 6, 2012, 3:31 PM), http://finance.yahoo.com/blogs/the-exchange/half-americans-set-die-without-193140015.html, *archived at* http://perma.cc/9L7N-V7UY.

requirement under the UFADAA and Delaware Act. Moreover, that may leave some fiduciaries frustrated in their attempts to catalog assets.

As for minimizing probate, litigation, and other administrative "hassles," the laws specify documentation that the fiduciary must furnish to the custodian to gain access and provide custodians with up to sixty days to comply with valid requests. This sixty-day requirement may present practical difficulties for the custodian; even if the custodian were able to automate the process of handling requests for access, it would nonetheless involve development and implementation expenses and additional staff to handle requests when the automated process does not fulfill the needs of the requestor.[182] Assuming ISPs were able to comply with the sixty-day rule without much practical difficulty or expense, the acts still leave open the question of how long an ISP is expected to preserve inactive accounts and their contents.

On their face, the laws would seem to minimize probate, litigation, and other administrative "hassles" by standardizing the process of granting fiduciary access and limiting the liability of custodians that comply with the acts in good faith. The Delaware Act is, in this respect, closer to meeting this goal than the UFADAA because it further provides for technological impracticality[183] and immunity should the custodian accidentally destroy the digital asset or account while acting in good faith.[184] On the other hand, the Delaware Act increases the likelihood that parties could try to litigate access issues because it provides for liability for damages, including "reasonable attorney's fees and costs, incurred in any action or proceeding that confirms the validity or authority of a fiduciary . . . or compels acceptance of the fiduciary's valid written request . . . ."[185] Jim Halpert—

182 Samantha D. Haworth, *Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act*, 68 U. MIAMI L. REV 535, 552–53 (2014).

183 12 DEL. C. § 5005(b) (2015).

184 *Id.* § 5006(g).

185 *Id.* § 5006(e)(2).

an attorney with DLA Piper and General Counsel of the State Privacy and Security Coalition, a group that represents Google, Yahoo, and Facebook, amongst others— pointed to this provision as one that could discourage small service providers from contesting written requests for access.[186]

More importantly, the laws cannot completely solve the issue of federal preemption. As a result, it is unclear at this stage exactly what the outer limits to access are. If a fiduciary requests access before the courts rule on whether federal laws prohibit the granting of access to a decedent's digital assets, then the ISP may understandably be hesitant to comply with the request. The Delaware Act more appropriately acknowledges that it is subject to the ECPA.[187] The UFADAA may benefit from such clarification instead of merely mirroring the language of the relevant federal statutes, which may change in meaning and force if the laws are amended.[188]

V. RECOMMENDATIONS

A uniform approach to fiduciary access to digital assets would be the most effective way to close the growing digital gap in estate administration, particularly given that most ISPs offer services crossing state and national borders.[189]

186 Telephone Interview with Jim Halpert, Director, State Privacy and Security Coalition (Oct. 16, 2014).

187 § 5005(b)(1).

188 *See, e.g.*, Modernize the Electronic Communications Privacy Act (ECPA), American Civil Liberties Union, http://www.aclu.org/feature/modernizing-electronic-communications-privacy-act-ecpa?redirect=technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa (last visited Apr. 20, 2015), *archived at* http://perma.cc/97CH-TNPV (arguing that the ECPA should be amended to provide more stringent limitations on access to electronic information and records, including that records should only be viewed in a "true emergency with informed consent and proper notice.").

189 While the issue of preemption is beyond the scope of this Note, it should be noted that legal and legislative changes will likely need to occur on a federal level to recognize the authority of fiduciaries for the purposes of accessing electronic communications and information. *See, e.g.*, Sandi S. Varnado, *Your Digital Footprint Left Behind at Death: An Illustration of*

Legislators, however, can clarify the UFADAA and the Delaware Act in several ways to better serve the goals articulated in this Note, to properly recognize differences between physical and digital assets, and to protect the privacy interests of third parties.

A. Changes to the UFADAA

First, the UFADAA should define the fiduciary's rights in terms of control, not access, in order to more clearly delineate the fiduciary's powers and to give the fiduciary meaningful powers to execute their duties. Currently, the UFADAA gives fiduciaries the "right to access," and the accompanying commentary states that section 8 "clarifies that the fiduciary has the same authority as the account holder."[190] In section 9, regarding compliance, custodians must honor fiduciary requests to access, control, or copy assets, with "control" defined in the commentary as the ability to "move (unless prohibited by copyright law) or delete" a digital asset.[191] It appears that the UFADAA's conception of access thus entails access, control (moving or deleting), and copying of assets, but the commentary language stating that the act is "enabling the fiduciary to do electronically what the account holder could have done electronically"[192] is overly broad, given that fiduciaries are still limited by their fiduciary obligations. In the same vein, the ULC used language that suggests that the fiduciary "steps into the shoes" of the decedent,[193] primarily to give the fiduciary relevant authorization and lawful consent under

Technology Leaving the Law Behind, 74 LA. L. REV. 719, 768 (2014) (arguing that both the CFAA and SCA should be amended to specifically provide that one who accesses a decedent's digital assets is in compliance with a state statute that will not violate either federal acts).

190 UFADAA, *supra* note 1, § 8 cmt.

191 *Id.* § 9 cmt.

192 *Id.*

193 *See id.* § 8 cmt. ("Subsection (b) reinforces the concept that the fiduciary 'steps into the shoes' of the account holder, with no more—and no fewer—rights.").

ECPA and computer access laws,[194] but this may mislead some fiduciaries into thinking that they can exercise more control than necessary to execute their duties.

While this broad language in the commentary could simply be omitted, this does not solve the larger problem that there is no concrete definition of access. In a memorandum to the UFADAA drafting committee on February 27, 2014, Chair Suzanne Brown Walsh noted that the committee needed to discuss whether to define the term "access."[195] While it appears that "access" was indeed used throughout in the final version, it is still not formally defined, because "the nature of the fiduciary's authority over the account will depend on the type of digital asset."[196] When explaining this reasoning in an article, Walsh reasons that "[a] fiduciary cannot impermissibly manage any asset under the fiduciary's control, including digital assets, rendering lengthy provisions delineating the scope of the fiduciary's authority over digital assets unnecessary."[197] But by using "manage" here, Walsh muddies the issue further—is she implying that a fiduciary *can* permissibly manage a digital asset in certain circumstances? If so, is managing a part of "access" or is it more? Language in the ULC's promotional materials only exacerbates this confusion: one document states that the act allows fiduciaries to "access, delete, preserve, and pass along digital assets as appropriate" under the uniform act,[198] even though distribution is mentioned nowhere in the act or its commentary. On the other hand, Naomi Cahn, the reporter on the ULC commission that drafted the UFADAA, explained "access" as a way of

194 *Id.* § 8 cmt.

195 *See* Walsh, *supra* note 15, at 445.

196 *Id.*

197 *Id.*

198 Uniform Law Commission, *Why Your State Should Adopt the Uniform Fiduciary Access to Digital Assets Act*, UNIF. LAW COMM'N, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/UFADAA%20-%20Why%20Your%20State%20Should%20Adopt%20-%20August%202014.pdf (last visited Apr. 20, 2015), *archived at* http://perma.cc/PXB2-GH5A.

emphasizing that the fiduciary can access information about a digital asset, but not the asset itself; if a bank has electronic statements belonging to the decedent, the fiduciary should be able to access that information to determine how much money is in an account, but does not then automatically get access to the money itself.[199] But in another context, such as email, where the underlying asset is information itself, it seems like the UFADAA is trying to give fiduciaries greater access to digital assets by allowing for requests to control and copy assets, in addition to access to information about the digital assets.

Access is a key point because it defines the scope of the fiduciary's powers. Walsh acknowledges that access may mean different things depending on the asset, but this is exactly why a stable definition is needed—fiduciaries and ISPs both need guidance in determining their rights and responsibilities across a variety of digital assets and accounts, and a uniform law should address this.

Here, the Delaware Act is instructive. The Delaware Act gives fiduciaries the ability "to exercise control over any and all rights in digital assets and digital accounts . . . ."[200] The UFADAA should adopt the language of control in describing the fiduciary's authority under the act, since it more accurately conveys the range of meaningful abilities the UFADAA seeks to give to the fiduciary—to access, control, or copy. By combining language from the Delaware Act and other sections of the UFADAA, "access" could be defined in the UFADAA as the:

> right and ability to exercise control over an account holder's digital asset, subject to other applicable law, and to the extent of the account holder's authority and the fiduciary's power under the law of this state other than this [act]. The fiduciary's control is limited to activities in furtherance of fiduciary duties.

199 Telephone Interview with Naomi Cahn, Professor, George Washington University Law School (Jan. 7, 2015).

200 12 DEL. C. § 5004(a).

TOS would be covered under "to the extent of the account holder's authority" and the definition makes clear that the fiduciary can only access the account in furtherance of fiduciary duties.[201] Moreover, in its current form, the UFADAA leaves open the question of who should decide the level of access, and what kind of access—login details, as compared to copies, for instance—should be granted. By giving fiduciaries control rather than just access, the UFADAA could give them the flexibility to make broader requests to ISPs as well as the ability to receive more information sooner.

It is logical for the UFADAA to utilize existing fiduciary duties to limit fiduciaries when accessing digital assets, but there needs to be further protection for third parties because of the volume and the interconnected nature of digital assets. As such, the UFADAA should contain language regarding the responsibilities of ISPs to create a "wall" around the decedent's account while the fiduciary accesses it. This restriction would allow an ISP to limit a deceased user's account so that the fiduciary could not access the digital assets of other users without its actions being construed as bad faith. This approach makes sense, since the fiduciary's obligations pertain only to the account holder's estate and belongings. Accordingly, in section 9, the UFADAA could include the following language: "In complying with a fiduciary's request in a record for access, control, or a copy of the asset to the extent permitted by copyright law, the custodian must restrict the fiduciary's access to only the account holder's digital assets, unless it would be technologically impracticable to do so."

This requirement is in accordance with the idea that fiduciary access must be in furtherance of fiduciary duties. For instance, if a Facebook user dies and the fiduciary wants to access the account in order to collect photographs that are of sentimental value, the fiduciary does not need to view status updates, posts, and photographs from other users that will appear in the decedent's newsfeed. This would be in

201 Walsh, *supra* note 15, at 442.

some ways the inverse of Facebook's memorialization feature, where the user's account is locked but can keep receiving posts and messages. In this case, the account no longer needs to be live to receive general updates from its Friends while the fiduciary assesses and saves digital assets. This would not apply to email accounts because email accounts only receive messages directed specifically at the account holder. Social media accounts, on the other hand, are often based around a feed or a real-time stream consisting of other users' social media activity.

The UFADAA is currently focused on fiduciaries, but it should not ignore the fact that the ISP, as custodian, is in the best position to collect a decedent's digital assets and exclude data that does not belong to the decedent. At the same time, the ISPs' technical control should not be translated directly into the power to make legal determinations that may impinge on a fiduciary's ability to execute his or her duties. In addition, the UFADAA should limit the fiduciary's authority if such limits are intended by a governing instrument or court order. Both the UFADAA and Delaware Act define governing instrument similarly to encompass a will, trust, court order, or other dispositive or nominative document, but only the Delaware Act provides that the fiduciary may exercise control "except as otherwise provided by a governing instrument or court order . . . ."[202] The UFADAA and the Delaware Act do not address whether there may be legitimate reasons to deny a fiduciary's request to deactivate or delete digital accounts, so should provide for governing instruments or court orders as limitations on the fiduciary's ability to act to minimize the risk of contravening the decedent's wishes or creating waste.

B. Changes to the Delaware Act

The Delaware Act should incorporate language similar to that proposed above for the UFADAA to limit fiduciary access only to the extent of fiduciary duties, and to require ISPs to create walls around the decedent's assets. Further,

[202] § 5004(a).

the UFADAA provides for immunity for custodians for "an act or omission done in good faith in compliance" with the Act, whereas the Delaware Act only provides immunity for actions. The Delaware Act should include omissions, especially in light of its imposition of liability for damages, since it is feasible that custodians may not receive a request because of technical errors and fail to act. The Delaware Act seems to already recognize that technical impracticalities and mistakes can occur in other provisions, so this addition would not be against the overall spirit of the act.

The Delaware Act further provides for liability for damages, including reasonable attorney's fees and costs incurred in any action or proceeding that confirms the validity or authority of a fiduciary to act, or compels acceptance of the fiduciary's valid written request under the act.[203] The UFADAA only provides that if a custodian fails to comply, the fiduciary may apply to the court for an order directing compliance.[204] In this case, the Delaware Act should follow the UFADAA, because liability for damages may discourage ISPs from challenging requests in situations where fiduciaries have too much or unnecessary access, which may compromise their abilities to protect the privacy interests of living users. In the short term, questions of preemption still remain unanswered by courts, which may justify a degree of caution on the ISP's part—after all, the SCA states that ISPs *may* disclose the contents of electronic communications, whereas the UFADAA and Delaware Act *compel* disclosure.

If liability for damages is insisted upon by states adopting the UFADAA, then they should consider specifying for how long an ISP is expected to preserve digital assets. Neither the UFADAA nor the Delaware Act does this. An estate usually takes six to ninth months to administer,[205] so

203 *Id.* § 5006(e)(2).

204 UFADAA, *supra* note 1, § 9(c).

205 *See, e.g.*, *Frequently Asked Question for Estate Administration*, HAMILTON COUNTY PROBATE COURT, http://www.probatect.org/services/faqs/forms_faqs_estate.html (last visited Apr. 20, 2015), *archived at* http://perma.cc/FX94-99GB (estimating that the "majority of estates

mandating that ISPs preserve digital assets and inactive accounts for at least 12 months after receiving a request should be sufficient, presuming most ISPs are able to comply with the sixty-day rule.[206]

VI. CONCLUSION

As more states consider adopting legislation that addresses fiduciary access to digital assets, a uniform approach that best balances the interests of consumers, ISPs, and fiduciaries must be put in place. In the longer term, legislation like the UFADAA and the Delaware Act could have significant impact on the development of digital history. Social media and new technologies are indelibly changing the way people relate to each other and leave legacies; indeed, it may become commonplace to mourn at a digital cemetery in the not-too-distant future. Fiduciary access to digital assets, then, may help preserve important aspects of a growing digital culture, in addition to allowing ISPs and those left behind to appropriately preserve valuable digital assets.

The ULC members involved in drafting the UFADAA seemed to conceive of their purpose as not drafting new law, but clarifying a legal issue.[207] While there are many good

should be finalized within 9 months of the date of the appointment of the fiduciary"); *Estate Administration Information*, FRANKLIN COUNTY PROBATE COURT, http://www.franklincountyohio.gov/probate/departments/estate_admin.cfm#How_Long_Should_it_Take (last visited Apr. 20, 2015), *archived at* http://perma.cc/654Z-4RGX ("The time it takes to administer an estate depends on each estate's circumstances. Some estates are administered in six to nine months.").

206 For example, the Nevada statute requires ISPs to preserve data for two years following a request. NEV. REV. STAT. § 143.188 (2014)

207 *Compare* Memorandum, John Gregory, to Suzanne Walsh and Naomi Cahn, Chair and Reporter, UFADAA Drafting Committee, *March Draft of the Fiduciary Access to Digital Asset Act (FADA)*, UNIF. LAW COMM'N (Mar. 16, 2014), *available at* http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2014mar16_FADA_Memo_Gregory.pdf, *archived at* http://perma.cc/MXF6-WQJV ("We are not creating 'new law' about the nature of assets generally or fiduciary powers generally. FADA will clarify a legal issue that could have been

reasons why the ULC wanted the UFADAA to operate within existing legal frameworks, this downplays how fundamentally different some digital assets are from physical assets. Uncertainty still surrounds issues relating to preemption, privacy, and contractual obligations, but practically, requiring the ISPs to limit fiduciary access to just the digital assets of the decedent will help facilitate the goals of (1) respecting privacy and observing federal and state laws relating to privacy; (2) honoring decedents' post-mortem wishes; (3) efficient disposal of digital assets and execution of fiduciary duties; and (4) minimizing probate, litigation, and other administrative "hassles." While ISPs have so far controlled almost all of the terms by which consumers use their products and services, increasing Internet use and volume of digital assets should prompt us to think critically and sustainably about how to allocate control between consumers and ISPs and provide parallel privacy protections for both living and dead users. The UFADAA and Delaware Act should be clarified in the ways put forward by this Note to minimize their impact on living account holders, so that the digital world might continue to be a place rich in value—socially, economically, sentimentally, or otherwise—and also to build a balanced system for dealing with the digital estates of users who pass away.

(and has been) argued either way until now"), *with* Bissett & Kauffman, *Surf the Evolving Web of Laws Affecting Digital Assets*, *supra* note 127, at 35 ("Because the primary purpose of the proposed [UFADAA] is to allow fiduciaries access to digital assets, the drafting committee's most important task was to create a legal right where none currently existed. That is, the drafting committee had to find a way for a deceased account holder to provide consent to a fiduciary.").