POSTHUMOUS PRIVACY, DECEDENT INTENT, AND POST-MORTEM ACCESS TO DIGITAL ASSETS

Alberto B. Lopez[*]

INTRODUCTION

In a book describing the history of the Internet published just before the turn of the century, an author loftily mused that the age of digitization sparked "social changes so profound their only parallel is probably the discovery of fire."[1] Comparing the digital age to the discovery of fire may involve a tiny bit of hyperbole, but the digital age has had an unquestionable impact on the way we live. The simple act of clicking a mouse or swiping a touchscreen has transformed us into individuals that look down at digital devices without regard to much else. Addressing the downward-looking trend, *The New York Times* published a blog post entitled "Distracted Walkers Pose Threat to Self and Others" that detailed the dangers of texting while walking.[2] Supporting the blog post's title, a recent scientific study found that texting while walking caused a 61% increase in "lateral deviation."[3] Statistically significant scientific results are valuable, but one need only walk down a street or in a shopping mall to conclude that texting while walking impairs what the study described as "executive function."[4]

Beyond its physiological effect, the digital revolution has triggered a cascade of legal consequences, both in and out of the courtroom. Digital media has had its most obvious legal impact on intellectual property law in cases like *Metro Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*;[5] however, the legal footprint created by the digital revolution is not confined to that domain.[6]

---

* Professor of Law, University of Alabama School of Law. The author thanks all of the individuals who patiently discussed the topic of this paper with him. Any errors are, of course, attributable to the author.

1 DAVID HUDSON, REWIRED: A BRIEF AND OPINIONATED NET HISTORY 7 (Carla Hall et al. eds., 1997) (quoting publisher Louis Rossetto in Wired magazine's debut issue).

2 Jane E. Brody, *Distracted Walkers Pose Threat to Self and Others*, N.Y. TIMES: WELL (Dec. 7, 2015), http://well.blogs.nytimes.com/2015/12/07/its-not-just-drivers-being-driven-to-distraction/?_r=0.

3 Eric M. Lamberg & Lisa M. Muratori, *Cell Phones Change the Way We Walk*, 35 GAIT & POSTURE 688, 689 (2012).

4 *Id.* at 688.

5 545 U.S. 913 (2005).

6 For information regarding the impact of file sharing on the Copyright Act, *see, e.g.*, The Honorable Marybeth Peters, Register of Copyrights, U.S. Copyright Office, Brace Memorial Lecture at the New York University School of Law: Copyright Enters the Public Domain (Apr. 29, 2004), *in* 51 J. Copyright Soc'y U.S.A. 701 (2004); *RIAA v. The People: Five Years Later*, Elec. Frontier Found. (Sept. 30, 2008), https://www.eff.org/wp/riaa-v-people-five-years-later#footnote91_ine688d (describing the difficulties

For example, ready access to and abuse of digital information prompted nearly all fifty states to enact criminal punishments for cyber-stalking and cyber-harassment.[7] But regardless of the specific area of law, the Newtonian relationship between technological advancement and the law is not, of course, new.[8] Orville and Wilbur Wright initiated numerous lawsuits seeking to protect the patent to their "flying machine" and the invention of the automobile generated traffic codes that transformed roads from a place occupied by pedestrians to a space reserved for cars.[9] In short, innovation has long led to litigation and legislation even if the innovation falls beneath fire in the order of importance.

Amidst an increasingly digitized world, one area of law has been largely resistant to change—the law of wills. The signature and witness requirements mandated by modern statutes of wills trace their origins back to the Statute of Wills of 1540, which was enacted during the reign of Henry VIII, as well as the Statute of Frauds of 1677.[10] Despite the centuries of inertia propelling some of the statutory requirements for valid execution of a will, the digital age has affected the interpretation of those requirements in isolated instances. For example, an Ohio court decided that a will written on a Samsung Galaxy tablet satisfied Ohio's signature and writing requirements, and a Tennessee court concluded that a "computer generated signature" met the state's signature requirement for due execution.[11] Legislatively, Nevada enacted a statute

---

associated with copyright enforcement); Evan Perez, *New Conservative Legal Challenge to NSA Phone Data Program*, CNN (June 5, 2015), http://www.cnn.com/2015/06/05/politics/nsa-phone-metadata-collection-court-challenge/index.html (outlining arguments that the NSA's metadata collection program challenges the protection afforded by the Fourth Amendment).

7 *See* Steven D. Hazelwood & Sarah Koon-Magnin, *Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis*, 7 INTL. J. CYBER CRIMINOLOGY 155, 159–61 (2013) (providing an extensive list of state statutes concerning cyberstalking and cyberharrassment and distinguishing between cyberstalking and cyberharrassment).

8 Isaac Newton was involved in an intellectual property dispute with Gottfried Wilhelm Leibniz over the invention of calculus. *See* Rose Eveleth, *Five Epic Patent Wars that Don't Involve Apple*, SMITHSONIAN (Aug. 27, 2012), http://www.smithsonianmag.com/smart-news/five-epic-patent-wars-that-dont-involve-apple-16729368/?no-ist.

9 *See, e.g.*, Wright Co. v. Herring-Curtiss Co., 211 F. 654 (2d Cir. 1914); Wright Co. v. Herring-Curtiss Co., 180 F. 110 (2d Cir. 1910); *see also* PETER D. NORTON, FIGHTING TRAFFIC: THE DAWN OF THE MOTOR AGE IN THE AMERICAN CITY (2008) (tracing the transformation of American street usage).

10 C. Douglas Miller, *Will Formality, Judicial Formalism, and Legislative Reform: An Examination of the New Uniform Probate Code "Harmless Error" Rule and the Movement Toward Amorphism, Part One: The Wills Act Formula, The Rite of Testation, and the Question of Intent: A Problem in Search of a Solution*, 43 FLA. L. REV. 167, 177 (1991) ("In comparison to other statutory law, the wills acts have proved to be extraordinarily resistant to change.").

11 Taylor v. Holt, 134 S.W.3d 830, 833 (Tenn. Ct. App. 2003); *see also,* Brad Dicken, *Judge Rules That a Will Written and Signed on Tablet Is Legal*, THE CHRONICLE-TELEGRAM (June 25, 2013), http://chronicle.northcoastnow.com/2013/06/25/judge-rules-will-written-signed-on-tablet-is-legal/ (explaining that a will written and signed on a tablet "will me[e]t the legal definition of a will in Ohio").

that validates "electronic wills" provided such wills contain the date, the testator's signature, and "one authentication characteristic of the testator."[12] While a few intersections between the law of wills and digital information can be unearthed, the law of wills and the digital age remain, for the most part, on parallel paths. Indeed, Nevada is the only state to recognize electronic wills by statute, and it did so fifteen years ago in 2001.[13]

Recently, however, the digital age has clashed with the law of wills in courtrooms and legislatures around the country.[14] As the world has become increasingly digitized, executors have encountered difficulty when seeking access to a decedent's digital assets that are stored in password-protected online accounts.[15] For example, the author of the international best seller *Pomegranate Soup*, Marsha Mehran, died unexpectedly and without explanation in Ireland.[16] Mehran's father, Abbas Mehran, sought to determine if his daughter left any literary works on her Google Chromebook after her tragic death. Hoping to unlock the Chromebook, Mr. Mehran sent four emails to Google seeking access to his daughter's account, but Google did not reply to any of the emails.[17] Eventually, Mr. Mehran hired an attorney and filed a petition in court asking for access to documents on his daughter's Google Drive account.[18] Following "several weeks of negotiation," Mr. Mehran obtained a CD from Google that included over 200 documents written by his

---

12 NEV. REV. STAT. § 133.085 (2014). For an examination of issues associated with digital wills, see Gerry W. Beyer & Claire G. Hargrove, *Digital Wills: Has the Time Come for Wills to Join the Digital Revolution?*, 33 OHIO N. U. L. REV. 865 (2007).

13 S. 33, 2001 Leg., 71st Sess. (Nev. 2001) (approving an act "providing for the use of electronic wills and electronic trusts").

14 *See, e.g.*, Naomi Cahn et al., *Digital Assets and Fiduciaries*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW (John A. Rothchild ed.) (forthcoming 2016), http://ssrn.com/abstract =2603398; Rebecca G. Cummings, *The Case Against Access to Decedents' Email: Password Protection as an Exercise of the Right to Destroy*, 15 MINN. J. L. SCI. & TECH. 897 (2014); James D. Lamm et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. MIAMI L. REV. 385 (2014); Jeehyeon Lee, Note, *Death and Live Feeds: Privacy Protection in Fiduciary Access to Digital Assets*, 2015 COLUM. BUS. L. REV. 654 (2015).

15 *See* Lee, *supra* note 14, at 664 (explaining that online service provider terms of service may be violated even where a decedent volunteered her login information to the fiduciary); Lamm et al., *supra* note 14, at 399–400 ("When a fiduciary uses an account holder's username and password . . . that fiduciary may risk criminal liability under federal and state criminal statutes."); *see generally* Cahn et al., *supra* note 14 (explaining that computer access does not necessarily mean access to the data where passwords and the data are encrypted).

16 Matt O'Brien, *Who Owns Your Digital Afterlife?*, SANTA CRUZ SENTINEL (Aug. 29, 2015), http://www.santacruzsentinel.com/business/20150829/who-owns-your-digital-afterlife ("An inquest [following Mehran's passing] . . . ruled out foul play but was otherwise inclusive, declaring: 'The medical cause of death is underlying diseases which are unknown.'").

17 *Id.*

18 *Id.* Mehran paid an attorney $1,000 to look into the matter, but soon looked for another attorney after learning that the attorney sought $10,000 for the representation. *Id.*

daughter.[19] The process began with the untimely passing of Mr. Mehran's daughter and ended with the delivery of the CD to Mr. Mehran, but took more than a year[20] —a statistic that accounts for neither the personal hardship endured nor the legal expense incurred during that period.

While Marsha Mehran's literary talent may have been unique, her usage of password-protected online accounts for storage and communication is anything but, and the challenges faced by individuals seeking access to those accounts are predictable. Password-protected online accounts are ubiquitous in the modern world, as individuals receive and pay bills, communicate via text or email, bank, store photos and documents, and game without a tangible analog in the physical world.[21] According to a 2007 Microsoft study, participants had twenty-five online accounts that required a password for access.[22] Following an individual's death, the decedent's personal representative may attempt to discover the online accounts used by the decedent, unearth the passwords to those accounts, and access those accounts in compliance with terms of service agreements that may or may not address account management at death.[23] Subscribers of online services may have trouble remembering their own logon information and passwords, let alone find such information for an unknown number of online accounts held by a decedent.

If a personal representative does, in fact, discover a decedent's online accounts and passwords, actual access to those accounts may violate state privacy laws. Statutory law in each state bars unauthorized access to a computer, accessing a computer without "effective consent," or some other similar phrase grounded in the notion of privacy.[24] Violations of such laws are

---

19 *Id.* The CD was mailed to Mehran's attorney who then mailed it to Australia. Mr. Mehran neither sought nor obtained his daughter's email messages. *Id.*

20 *Id.* Marsha Mehran died in April 2014 and her father received the CD in June 2015 or at some point shortly thereafter. *Id.*

21 *See generally* Dinei Florêncio & Cormac Herley, *A Large-Scale Study of Web Password Habits*, INTERNATIONAL WORLD WIDE WEB CONFERENCE COMMITTEE (2007), http://www2007.org/papers/paper620.pdf (finding that the average user has about 25 password protected web accounts).

22 *Id.*

23 Jena L. Levin & John T. Brooks, *Administration of Trusts and Estates in the Digital Age*, WEALTHMANAGEMENT.COM (Dec. 1, 2015), http://wealthmanagement.com/estate-planning/administration-trusts-and-estates-digital-age ("Terms of Service (TOS) agreements for digital accounts . . . are typically silent regarding fiduciary access or simply prohibit third parties from accessing accounts altogether . . . .").

24 MD. CODE ANN., CRIM. LAW § 7-302(c)(1)(i) (2016) ("A person may not . . . without authorization: access, attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer network, computer control language, computer, computer software, computer system, computer service, or computer database."); TEX. PENAL CODE ANN. § 33.02(a) (2015) ("A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner."). For a list of state privacy laws, see *Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (last updated May 12, 2016).

deemed criminal offenses punishable by monetary fines and/or prison time.[25] While the statutory protections may be primarily aimed at computer hacking, a personal representative's act of accessing a decedent's online account in the absence of consent seemingly runs afoul of the sweeping language of state privacy laws.[26] As a result, the threat of criminal sanction, even if remote, creates a disincentive for a representative to seek access to a decedent's online accounts. To account for whatever degree of risk is posed by state privacy laws, estate planners recommend preparing a list of online accounts and passwords prior to death to provide evidence that a personal representative's access has been authorized by the decedent.[27] Reflecting market demand for post-mortem access mechanisms, online businesses that provide post-mortem digital asset services are in no short supply.[28] Nevertheless, most individuals die without any estate planning; therefore, many, if not most, personal representatives are unlikely to have much information about the totality of a decedent's online presence.[29]

As an alternative, a personal representative may submit a request to an online service provider for access to the decedent's account and a copy of information stored in the account.[30] Online service providers, however, are reluctant to permit access to and the subsequent transfer of digital information for fear of violating the Stored Communications Act ("SCA"), which is a portion of the larger Electronic Communications Privacy Act.[31] Section

---

25 *See, e.g.*, MD. CODE ANN., CRIM. LAW § 7-302(d)(1) (2016) (imposing a fine of up to $1,000 and/or a prison term not exceeding three years); TEX. PENAL CODE ANN. § 33.02(b) (2015) (designating the offense as a "Class B misdemeanor").

26 *See, e.g.*, VA. CODE ANN. § 18.2-152.5 (2016) ("A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit, or any other financial or identifying information . . . relating to any other person.").

27 *See, e.g.*, Mary Randolph, *Access to Online Accounts: Helping Your Executor and Loved Ones*, NOLO, http://www.nolo.com/legal-encyclopedia/access-online-accounts-helping-executor-35013.html (last visited Aug. 22, 2016).

28 *See* Evan Carroll, *RIP Digital Legacy Startups*, THE DIGITAL BEYOND (Mar. 21, 2014), http://www.thedigitalbeyond.com/2014/03/rip-digital-legacy-startups/ (cataloging the success and failure of various online businesses that handle digital assets).

29 Press Release, Lawyers.com, *Majority of American Adults Remain Without Wills, New Lawyers.com Survey Finds* (Apr. 3, 2007), http://press-room.lawyers.com/majority-of-american-adults-remain-without-wills.html. *But see* Mary Louise Fellows et al., *Public Attitudes About Property Distribution at Death and Intestate Succession Laws in the United States*, 1978 AM. B. FOUND. RES. J. 319, 336-39 (1978) (suggesting that the rate of testation may be greater than generally accepted).

30 *See, e.g.*, Ajemian v. Yahoo!, Inc., 987 N.E.2d 604, 608–09 (Mass. App. Ct. 2013) (discussing a request submitted by co-administrators of the decedent's estate for access to the decedent's Yahoo! email account.)

31 Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2701–12 (2012)); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

2702(a)(1) of the SCA states "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[32] The SCA contains exceptions that permit voluntary disclosure,[33] but transferring the contents of an online account to a personal representative during estate administration is not one such exception.[34] While it may protect an account holder's privacy interests during the account holder's life, the SCA creates an additional legal obstacle to post-mortem data acquisition via disclosure limitations it places on service providers.[35]

The challenges encountered by a personal representative may be daunting, but accessing online accounts could prove critical due to the potential value a decedent's digital assets. A 2012 Wall Street Journal article reported that Americans valued their digital assets at over $55,000.[36] Similarly, a worldwide McAfee study released in 2013 concluded that the value of digital assets stored on digital devices exceeded $35,000.[37] The types of digital assets held by individuals ranged from individual memories, valued at over $17,000, to career information and entertainment files, valued at over $4,000 and $1,000, respectively.[38] Though it may be difficult to believe that personal memories have monetary values measured in the thousands of dollars, there is no question that digital property can be surprisingly valuable. The 2008 edition of the Guinness Book of World Records identified an "asteroid" as "The Most Expensive Virtual Object" at a purchase price of $100,000, which eventually increased in value to $1 million and provided a monthly income for its owner.[39] Most people, of course, are not engaged in online transactions to such an extreme. But even if the actual dollar value assigned to an individual's digital assets in McAfee's study were only 10% of the study's reported value, the monetary value would still amount to $3,500.[40] Such a figure is not

---

32 18 U.S.C. § 2702(a)(1) (2012).

33 *Id.* § 2702(b).

34 For an argument that personal representatives should be included among the exceptions, see Natalie M. Banta, *Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death*, 83 FORDHAM L. REV. 799, 840–42 (arguing that the exception for agents of a recipient of an electronic communication should apply to estate representatives).

35 18 U.S.C. § 2702(a) (2012).

36 Kelly Greene, *Passing Down Digital Assets*, WALL ST. J. (Aug. 31, 2012), http://www.wsj.com/articles/SB10000872396390443713704577601524091363102.

37 Robert Siciliano, *How Do Your Digital Assets Compare?*, MCAFFEE: CONSUMER BLOG (May 14, 2013), https://blogs.mcafee.com/consumer/digital-assets/.

38 *Id.*

39 Simon Hill, *Most Expensive Items Ever Sold in an MMO*, ALTERED GAMER (Apr. 18, 2012), http://world-of-warcraft.alteredgamer.com/wow-other-items/29070-most-expensive-items-ever-sold-in-an-mmo/.

40 *See* Siciliano, *supra* note 37.

only likely to be significant for individual account holders, but is also representative of the vast amount of wealth locked behind password-protected online accounts when considered in the aggregate of online users.

Recognizing the legal obstacles that impede access to the potential value stored in a decedent's online accounts, the Uniform Law Commission ("ULC") began to develop a proposal that would provide fiduciaries with access to a decedent's digital assets in May 2011.[41] One year later, the ULC circulated a draft of the proposal and sought reaction from interested parties.[42] In turn, a broad spectrum of groups and individuals commented on the proposal, including the American Civil Liberties Union ("ACLU") and other consumer advocacy groups.[43] Following consideration of positive and negative comments, the ULC promulgated the Uniform Fiduciary Access to Digital Assets Act ("UFADAA") in July 2014.[44] The ULC's model act granted personal representatives with broad access to a decedent's digital assets in the absence of an express prohibition by the decedent.[45] As a measure of the regulatory necessity, twenty-six states introduced UFADAA bills into their state legislatures during their respective 2014-2015 sessions.[46] Thus, the law

---

41 Letter from Gene H. Hennig, Minn. Comm'r, Unif. Law Comm'n, to Comm'r Harriet Lansing, Chair, Comm. On Scope and Program, Unif. Law Comm'n (July 5, 2011), http://www.uniformlaws.org/Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets [hereinafter Hennig letter] (proposing to extend access to fiduciaries other than a personal representative of a decedent's estate, such as a holder of a power of attorney or conservator). This paper is limited to an examination of access to digital assets for a personal representative of an estate; therefore, issues associated with the other fiduciaries covered by the proposal will neither be identified nor examined.

42 Memorandum from Suzanne Brown Walsh and Naomi Cahn to the Drafting Comm. on Fiduciary Access to Dig. Assets (FADA) (Nov. 11, 2012), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2012nov11%20_FADA_Mtg_IssuesMemo.pdf.

43 *See, e.g.*, Letter from Allison S. Bohm, Advocacy and Policy Strategist, Am. Civil Liberties Union Found. to Suzanne Brown Walsh, Chair, Unif. Law Comm'n and Professor Naomi Cahn, Reporter, Unif. Law Comm'n (July 3, 2013), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jul3_FADA_Comments_ACLU.pdf [hereinafter Bohm Letter]; Letter from Richard O. Rash and Diane H. Rash to Suzanne Brown Walsh, Principal, Cummings & Lockwood LLC (July 5, 2013), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jul5_FADA_Comments_Rash.pdf [hereinafter Rash Letter]; Letter from Steve DelBianco, Exec. Dir., NetChoice, Carl M. Szabo, Policy Counsel, NetChoice, and James J. Halpert, Gen. Counsel, State Privacy & Security Coalition to Suzanne Brown Walsh (July 8, 2013), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013jul_FADA_NetChoice_Szabo%20et%20al_Comments.pdf [hereinafter DelBianco, et al. Letter].

44 UNIF. FIDUCIARY ACCESS TO DIG. ASSETS ACT (UNIF. LAW COMM'N 2014), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2014_UFADAA_Final.pdf [hereinafter UFADAA].

45 *Id.* § 4.

46 *See Legislation*, UNIF. LAW COMM'N, http://uniformlaws.org/Legislation.aspx?title=Fiduciary+Access+to+Digital+Assets (use navigation tools to show "All" Bill Dates by state) (last visited Aug. 20, 2016).

of wills was set to change at an unfathomable pace compared to its historically glacial rate of change.

Whatever momentum had propelled UFADAA in mid-2014, however, quickly dissipated—or perhaps more accurately, came to a screeching halt.[47] A number of the parties that had submitted comments on UFADAA during its drafting stage launched lobbying efforts to block passage of the model law.[48] The basic objection focused on privacy-related concerns associated with a personal representative's ability to access information in an online account by default.[49] Furthermore, some big tech companies, like Yahoo!, asserted that permitting such access violated the terms of service agreements between the company and the deceased account holder.[50] The lobbying efforts of those against passage proved most persuasive, as twenty-five of the twenty-six UFADAA based bills considered by state legislatures during the 2014-2015 legislative sessions failed to become law.[51]

Rather than negotiate with the ULC to seek a compromise that addressed its concerns, one of the proposal's chief opponents, NetChoice, drafted its own proposal as an alternative to the ULC's work product.[52] NetChoice describes itself as "an association of eCommerce businesses and online consumers who share the goal of promoting convenience, choice, and commerce on the net."[53] The phrase "an association of eCommerce businesses" understates the influence likely wielded by certain of its members, which includes Google, Facebook, Yahoo!, eBay, PayPal, and other weighty tech organizations. NetChoice's proposal, The Privacy Expectation Afterlife and Choices Act (PEAC),[54] occupies the opposite end of the privacy spectrum

---

47 Morgan M. Weiner, *Opposition to the Uniform Fiduciary Access to Digital Assets Act*, NAT'L L. REV. (Jul. 21, 2015), http://www.natlawreview.com/article/opposition-to-uniform-fiduciary-access-to-digital-assets-act.

48 *Id.*; Carly Ziegler, *Fiduciary Access to Digital Assets and Accounts—Uniform Fiduciary Access to Digital Assets Act "UFADAA"*, NAT'L L. REV. (Oct. 3, 2014), http://www.natlawreview.com/article/fiduciary-access-to-digital-assets-and-accounts-uniform-fiduciary-access-to-digital-.

49 Ziegler, *supra* note 48.

50 *Id.*; Bill Ashworth, *Your Digital Will: Your Choice*, YAHOO! (Sept. 15, 2014), https://yahoopolicy.tumblr.com/post/97570901633/your-digital-will-your-choice.

51 Weiner, *supra* note 47. For a list of states that introduced a bill based upon the Committee's proposal, *see Legislation*, UNIF. LAW COMM'N, *supra* note 46.

52 *See* Anne W. Coventry & Karin Prangley, *Status of the Uniform Fiduciary Access to Digital Assets Act. Not Enacted Anywhere . . . Yet.*, AM. BAR ASS'N. (May 20, 2015), http://www.americanbar.org/content/dam/aba/publishing/rpte_ereport/2015/3-May/practice_alert.authcheckdam.pdf; Letter from Carl Szabo, Policy Counsel, NetChoice, to Matthew Shepherd, Representative, Ark. House of Representatives (Feb. 18, 2015), https://netchoice.org/wp-content/uploads/NetChoice-Opposition-to-AR-HB-1362.pdf.

53 NETCHOICE, https://NetChoice.org/ (last visited Aug. 26, 2016).

54 *Privacy Expectation Afterlife and Choices Act (PEAC)*, NETCHOICE, http://NetChoice.org/library/privacy-expectation-afterlife-choices-act-peac/ [hereinafter PEAC].

when compared to the ULC's model law.[55] Under PEAC, a personal representative does not have default access to a decedent's digital assets, but may gain access under specific circumstances, such as when a court issues an order directing access.[56] However, unlike the widespread introduction of the ULC's law into state legislatures, PEAC has only been placed on the legislative agenda in four states thus far, and only one of those states, Virginia, enacted a form of the PEAC in 2015.[57] Thus, ironically, the number of states that have codified PEAC and UFADAA to date is equal.

Although the ULC's 2014 effort stalled in state legislatures around the nation, it did not permit PEAC to monopolize legislative attention. Within one year of passing its 2014 model act, the ULC passed a revised version of the Uniform Fiduciary Access to Digital Assets Act ("RUFADAA").[58] The ULC responded to the criticisms aimed at the 2014 act by enacting provisions more closely aligned with PEAC on the issue of privacy of digital assets in comparison its predecessor.[59] More fundamentally, the evolution of UFADAA into RUFADAA seemed to occur without much consideration of the decedent's possible interest in post-mortem privacy of account information.[60] Nevertheless, RUFADAA has been placed on the legislative agenda in thirty-one states.[61] Furthermore, in a strange twist of legislative fate, NetChoice now supports RUFADAA and describes its provisions as "privacy-centric."[62] Some of UFADAA's other opponents, however, have yet

---

55 *Compare id.*, *with* UFADAA, *supra* note 44. *See also* Coventry & Prangley, *supra* note 52.

56 PEAC, *supra* note 54, § 1(B)(c).

57 *See* VA. CODE ANN. § 64.2-109-15 (2015); *see also* Assemb. B. 691, 2015-2016 Leg. Sess. (Cal. 2016), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB691; H.B. 2647, 78th Or. Leg. Assemb., Reg. Sess. (Or. 2015), https://olis.leg.state.or.us/liz/2015R1/Downloads/MeasureDocument/HB2647; *Task Force on Digital Information Privacy Summary of Proceedings*, Task Force on Dig. Info. Privacy (Wyo. 2014), http://legisweb.state.wy.us/interim Committee/2014/SDIMIN0731.pdf. For more information on Virginia's enactment of PEAC, *see generally* Mark Obenshain & Jay Leftwich, *Protecting the Digital Afterlife: Virginia's Privacy Expectation Afterlife and Choices Act*, 19 RICH. J. L. & PUB. INT. 39 (2015).

58 REVISED UNIF. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (2015) (UNIF. LAW COMM'N 2015), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2015_RUFADAA_Final%20Act_2016mar8.pdf [hereinafter RUFADAA].

59 *Compare id.*, *with* UFADAA, *supra* note 44.

60 *Compare* UFADAA, *supra* note 44, *with* RUFADAA § 6, *supra* note 58.

61 *Fiduciary Access to Digital Assets Act, Revised (2015)*, UNIF. LAW COMM'N, http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20%282015%29 (last accessed Aug. 26, 2016).

62 Two-Pager on the Uniform Fiduciary Access to Digital Assets Act (Revised), NETCHOICE, https://NetChoice.org/wp-content/uploads/Uniform-Fiduciary-Access-to-Digital-Assets-Act-Revised-2-pager.pdf (last accessed Aug. 28, 2016) [hereinafter NetChoice Two-Pager].

to stake out legislative positions on RUFADAA;[63] therefore, another legislative battle over the issues of access to and disclosure of the contents of a decedent's digital assets remains a distinct possibility.

The purpose of this Article is to inject consideration into the legislative calculus that has been largely absent from the debate engulfing RUFADAA and PEAC—a decedent's interest in posthumous privacy—and to integrate that interest into proposals regarding post-mortem access to digital assets. Part I canvasses the history of the legal response to the issue of post-mortem access to digital assets from the first statutes to the current model statutes, RUFADAA and PEAC. Traditional law posits that an individual does not have an interest in privacy after death, but Part II contends that an individual does, in fact, have such an interest. To support this assertion, Part II argues that the justifications for the privacy protections afforded to decedents under the Health Insurance Portability and Accountability Act of 1996 ("HIPPA") and the Freedom of Information Act ("FOIA") warrant the recognition of posthumous privacy for digital assets. Because current proposals place focus on the interests of online service providers rather than the intent for posthumous privacy, Part III refocuses legislative analysis to include decedent intent. Factoring posthumous privacy into the regulatory equation yields a default rule of non-disclosure for intestate estates and a default rule of disclosure if a provision for disclosure is included in a testator's will. Finally, the Article concludes that breaking from the traditional limitation of privacy to consider decedent intent regarding post-mortem access to and disclosure of digital assets effectuates the fundamental maxim of the law of wills: honoring a decedent's intent.

I. THE EVOLUTION OF THE LAW GOVERNING POST-MORTEM ACCESS TO DIGITAL ASSETS

Aided by the clarity of hindsight, the clash of digitization with the administration of decedent estates appears to have been inevitable. On one hand, the metamorphosis from the shoebox to the cloud for storage purposes not only permitted paperless business transactions, but has also allowed account holders to retain valued property in password-protected online accounts for extended periods of time.[64] Whatever the value of online property happens to be, even if the value is entirely subjective it is affixed to *property* that individuals may want to transfer at death.[65] Photos stored in one's Flickr[66]

---

63 *See* Levin & Brooks, *supra* note 23 (writing that although some online service providers support the ULC's revisions, "[n]othing is guaranteed . . . and it's still unclear whether the consumer privacy groups will come on board").

64 *See* Siciliano, *supra* note 37.

65 *Id.*

66 *About Flickr*, FLICKR, https://www.flickr.com/about (last visited Aug. 10, 2016).

account are unlikely to sell on the open market, but an individual may wish to pass those photos to others at death. After the death of an account holder, personal representatives have a fiduciary duty to pay a decedent's debts, collect a decedent's property, and distribute such property under the terms of a decedent's will or according to a state's scheme for intestacy.[67] As paperless transactions increased due to the efficiency of online transactions and environmental concerns,[68] personal representatives found it increasingly necessary to access online accounts during estate administration. However, despite the converging paths of online storage and estate administration, the issue of post-mortem access to online accounts failed to capture legislative attention until recently.[69] This Part traces the evolution of the legal response to the problem of post-mortem access to a decedent's digital assets from the first state statutes to the current model acts slated for broad consideration.

A. *First and Second Generation State Statutes*

The legislative impetus for the first state statute to address access to a decedent's online accounts illustrates the impediment to estate administration caused by the transition from an offline to an online world. Following the death of her husband and business partner, a surviving wife sought access to her late husband's email account to discover information related to their business.[70] The Internet service provider, however, refused to provide access to the email account.[71] In response to the problem faced by the surviving spouse, who happened to be a constituent of the sponsoring legislator, a Connecticut state legislator introduced "An Act Concerning Access to a Decedent's Email Accounts" to the state legislature in 2005.[72] The proposal required an Internet service provider "to provide access to electronic mail accounts and other electronic data in the name of a deceased person" after receiving evidence of

---

67 *See, e.g.*, COLO. REV. STAT. § 15-12-703 (2016); IND. CODE § 29-1-13-1 (2016); KY. REV. STAT. ANN. § 395.001 (West current through the end of the 2016 regular session); S.C. CODE ANN. 1976 § 62-3-703 (2009 & Supp. 2015); WIS. STAT. § 857.03 (2016).

68 *See, e.g.*, *Overview*, PAYITGREEN, http://www.payitgreen.org/business (last visited Aug. 31, 2016) (encouraging businesses and individuals to engage in paperless transactions as an environmental measure).

69 *See* Jim Lamm, *Delaware Enacts Fiduciary Access to Digital Assets Act*, DIGITAL PASSING (Aug. 27, 2014) http://www.digitalpassing.com/2014/08/27/delaware-enacts-fiduciary-access-digital-assets-act/; *see also, e.g.*, MICH. H. JUDICIARY COMM., LEGISLATIVE ANALYSIS OF H.B. 5366-5370, at 2 (Nov. 6, 2014), http://www.legislature.mi.gov/documents/2013-2014/billanalysis/House/pdf/2013-HLA-5366-EB0C233D.pdf.

70 CONN. JUDICIARY COMM., REPORT ON AN ACT CONCERNING ACCESS TO DECEDENT'S ELECTRONIC MAIL ACCOUNTS, S.B. 262 (Conn. 2005), https://www.cga.ct.gov/2005/jfr/s/2005SB-00262-R00JUD-JFR.htm.

71 *Id.*

72 *Id.*

the account holder's death.[73] Although the proposal became law, the language of the final public act excluded the phrase "other electronic data," thereby limiting the disclosure requirement to email accounts only.[74] Nevertheless, Connecticut General Statute § 45a-334a represents the first legislative response to the problem of gathering information about a decedent stored in an online account.[75]

Connecticut's foresight did not cross many state lines, as only two states followed its lead—and even then, not until a full two years had passed.[76] In 2007, the Indiana legislature considered a bill that required a "custodian" to provide "access to or copies of any documents or information of the deceased person stored electronically by the custodian" after receiving proof of the user's death.[77] Notably, the legislative synopsis of the bill informed legislators that "[e]lectronic documents are estate property," which is one of the earliest legislative denominations of online assets as "property."[78] During that same year, Rhode Island state legislators contemplated a bill that required an "electronic mail service provider" to give a personal representative "access to or copies of the contents of the electronic mail account" of a decedent if sufficient proof of the account holder's death is furnished to the service provider.[79] Both measures received unanimous votes of approval and became part of the statutory codes of each state.[80]

While they may have been prescient, the first generation statutory responses in Connecticut, Indiana, and Rhode Island are now criticized for being out-of-date for the modern digital world.[81] Indeed, the growth in paperless transactions, the proliferation of online storage, and the ever-increasing spectrum of online services make the requirement of disclosing only the contents of an email account seem antiquated. At the time of Connecticut's legislation

---

73 S.B. 262, 2005 Gen. Assemb., Jan. Sess. (Conn. 2005), https://www.cga.ct.gov/2005/tob/s/2005SB-00262-R00-SB.htm.

74 2005 Conn. Pub. Acts 05-136, https://www.cga.ct.gov/2005/ACT/PA/2005PA-00136-R00SB-00262-PA.htm; *see also* Matthew D. Glennon, *A Call to Action: Why the Connecticut Legislature Should Solve the Digital Asset Dilemma*, 28 QUINNIPIAC PROB. L. J. 48, 50–54 (2014).

75 CONN. GEN. STAT. ANN. § 45a-334a (West 2015).

76 *See* IND. CODE § 29-1-13-1.1 (2015) (under the heading of "Electronically stored documents of deceased"); R.I. GEN. LAWS § 33-27-3 (2015) (entitled "Access to a decedent's electronic mail").

77 S.B. 212, 2007 Gen. Assemb., 1st Reg. Sess. (Ind. 2007), http://www.in.gov/legislative/bills/2007/IN/IN0212.1.html.

78 *Id.*

79 H.B. 5647, 2007 Gen. Assemb., Jan. Sess. (R.I. 2007), http://webserver.rilin.state.ri.us/BillText/BillText07/HouseText07/H5647A.pdf; S.B. 0732, 2007 Gen. Assemb., Jan. Sess. (R.I. 2007), http://webserver.rilin.state.ri.us/BillText/BillText07/SenateText07/S0732.pdf.

80 IND. CODE § 29-1-13-1.1 (2015) (under the heading of "Electronically stored documents of deceased"); R.I. GEN. LAWS § 33-27-3 (2015) (entitled "Access to a decedents' electronic mail").

81 Lamm, *supra* note 69 (noting that an additional criticism is the statutory limitation providing access to personal representatives only, which omits others in fiduciary relationships that might need access to information stored in online accounts).

in 2005, for example, Facebook had only one million users.[82] A decade later, one billion people logged onto Facebook in a single day on August 24, 2015.[83] Recognizing the shift in the online world, a Connecticut legislator recently introduced a bill to commission a study of access to decedent "electronic accounts" in conjunction with estate administration.[84] The phrase "electronic accounts" comprehends broader access concerns than those animating Connecticut's current law limiting access to email accounts.[85] Nonetheless, legislators can hardly be faulted for failing to foresee that the online world would expand to the point that one billion people would use an online social network in one day. To that end, outdated statutes are not necessarily useless statutes—a personal representative still has the ability to discover debts, creditors, or property stored in an email account that might ease the administration of a decedent's estate.[86]

After a three-year hiatus, the issue of post-mortem access again garnered legislative attention as the second generation of statutes went into the books between 2010 and 2014. Oklahoma's statute, enacted in 2010, provides a personal representative with the authority "to take control of, conduct, continue, or terminate any accounts of a deceased person on any social networking website, any microblogging or short message service website or any e-mail service websites."[87] One year later, Idaho granted access to personal representatives using similar statutory language.[88] In 2014, Louisiana added to the second generation of statutes by requiring "any person that electronically stores, maintains, manages, controls, operates, or administers the digital accounts of a decedent" to "transfer, deliver, or provide . . . access or possession of any digital account" after receiving proof of the account holder's death.[89] According to the statute, a "digital account" includes everything from an email account to a "financial account Internet website."[90] Contemporary

---

82 *Our History*, FACEBOOK: NEWSROOM, http://newsroom.fb.com/Company-Info/ (use website controls to navigate to "Dec. 1, 2004" on the timeline) (last accessed Aug. 10, 2016).

83 *Id.* (use website controls to navigate to "Aug. 24, 2015" on the timeline).

84 H.R. 5227, 2013 Gen. Assemb., Jan. Sess. (Conn. 2013), https://www.cga.ct.gov/2013/TOB/H/2013HB-05227-R00-HB.htm.

85 *See id.* ("[The] study [shall] include, but not be limited to, an examination of the executor's or administrator's ability to distribute assets maintained in an electronic financial account by the decedent.").

86 *See* Molly Wilkens, *Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?*, 62 HASTINGS L. J. 1037, 1046–47 (2011) ("Without access to, or knowledge of, relevant email accounts, awareness of online financial transactions could disappear entirely upon the death of the account holder.") (footnote omitted).

87 58 OKLA. STAT. ANN. tit. 58, § 269 (West 2016).

88 IDAHO CODE § 15-3-715 (2015).

89 LA. CODE CIV. PROC. ANN. art. 3191(D)(1) (2015). The personal representative must gain access within thirty days of providing evidence of the account holder's death. *Id.*

90 *Id.* art. 3191(H) (2015) ("[T]he term 'digital account' shall include any account of the decedent on any social networking Internet website, web log Internet website, microblog service Internet website, short message service Internet website, electronic mail service Internet website, financial account Internet

online activity encompasses far more than sending and receiving emails; therefore, the second generation of statutes more accurately reflect the modern online world when compared to their statutory predecessors.[91]

Despite generational differences in the types of online accounts covered, both first and second-generation statutes attracted considerable legislative support at all stages of the legislative process.[92] The favorable reception, of course, does not mean that bills were not subjected to modification during the numerous hearings, debates, and votes that comprise typical legislative procedures.[93] To the contrary, several second-generation proposals were amended prior to final passage.[94] Nevertheless, each of the bills became law

website, or any similar electronic services or records, together with any words, characters, codes, or contractual rights necessary to access such digital assets and any text, images, multimedia information, or other personal property stored by or through such digital account.").

91 Two more state statutes were enacted between 2010 and 2014. However, each statute falls short of granting wide access for purposes of estate administration. Virginia Code § 64.2-110, enacted in 2013, provides a personal representative of a minor's estate with access to a "digital account," but does not grant equivalent access to the personal representative of an adult decedent. VA. CODE ANN. § 64.2-110 (2015). Nevada's provision, enacted in 2014, permits a personal representative "to direct the termination of any account of the decedent," which includes emails accounts as well as social networking accounts. NEV. REV. STAT. § 143.188 (2015). As a result, Nevada's law does not permit access for purposes of disclosing account contents as part of estate administration. The personal representative merely possesses the power to terminate the digital account.

92 *See, e.g.*, JUDICIARY COMM., SESS. YEAR 2005, VOTE TALLY SHEET, S.B. 212 (Conn. 2005), https://www.cga.ct.gov/2005/ts/s/2005SB-00262-R00JUD-CV76-TS.htm; H. COMM. ON JUDICIARY, 115TH GEN. ASSEMB., COMM. REP. ON S.B. 212 (Ind. 2007), http://www.in.gov/legislative/bills/2007/PDF/HCRP/DP021201.001.pdf; S. COMM. ON JUDICIARY, 115TH GEN. ASSEMB., COMM. REP. FOR S.B. 212 (Ind. 2007), http://www.in.gov/legislative/bills/2007/PDF/SCRP/DP021201.001.pdf; H. JUDICIARY, RULES, & ADMIN. COMM., 2011 SESS., MINUTES – MONDAY, FEB. 23, 2011 (Idaho 2011), https://legislature.idaho.gov/sessioninfo/2011/standingcommittees/hjudmin.pdf; S. JUDICIARY & RULES COMM., 2011 SESS., MINUTES – MONDAY, FEB. 7, 2011 (Idaho 2011), https://legislature.idaho.gov/sessioninfo/2011/standingcommittees/sjudmin.pdf; H.J. 28, 2014 REG. SESS., at 37–38 (La. 2014), http://house.louisiana.gov/H_Journals/H_Journals_All/2014_RSJournals/14RS%20-%20HJ%200428%2028.PDF; S.J. 5, 2014 REG. SESS., at 7 (La. 2014), http://senate.la.gov/sessioninfo/journals/2014/03-18-2014.pdf

93 *See, e.g.*, S. JUDICIARY & RULES COMM., S.B. 1044 (Idaho 2011), http://legislature.idaho.gov/legislation/2011/S1044.htm; NEV. LEG., 2013 SESS., S.B. 131 (2013), http://www.leg.state.nv.us/Session/77th2013/Reports/history.cfm?ID=338.

94 *See* bill information cited *supra* note 93.

with little to no legislative opposition.[95] In fact, all but one of the bills granting post-mortem access to online accounts received unanimous support.[96] Counting the total yea and nay votes cast in state legislatures during votes on both first and second-generation statutes yields a total of 743 yeas and 18 nays.[97] The eighteen nay votes were cast against the proposal debated in Louisiana's state legislature, and even there, the 18 votes against enactment were dwarfed by the105 votes in favor of Louisiana's bill.[98]

The bipartisan support for access to a decedent's online accounts is not only eye opening in terms of a one sided tally, but is significant given the infrequency of such cooperation in today's political environment. One reason for the overwhelming support of the access measures can be found in the fiscal impact statements associated with each legislative bill.[99] States that

---

95 CONN. GEN. ASSEMB., SESS. YEAR 2005, VOTE FOR SB-262 ROLL CALL NO. 289 (2005), https://www.cga.ct.gov/2005/vote/h/2005HV-00289-R00SB00262-HV.htm (143 Yeas, 0 Nays); CONN. GEN. ASSEMB., SESS. YEAR 2005, VOTE FOR SB-262 SEQUENCE NO. 193 (2005), https://www.cga.ct.gov/2005/vote/s/2005SV-00193-R00SB00262-SV.htm (34 Yeas, 0 Nays); IND. H.R., 115TH GEN. ASSEMB., ROLL CALL 356 (2007), http://www.in.gov/legislative/bills/2007/PDF/Hrollcal/0356.PDF.pdf (96 Yeas, 0 Nays); IND. S., 115TH GEN. ASSEMB., ROLL CALL NO.: 112 (2007), http://www.in.gov/legislative/bills/2007/PDF/Srollcal/0112.PDF.pdf (48 Yeas, 0 Nays); 134 J.H.R. NO. 65, 2007 SESS., at 99 (R.I. 2007), http://webserver.rilin.state.ri.us/Journals07/HouseJournals07/HJournal6-22.pdf (60 yeas, 0 Nays); 134 S.J. NO. 58, 2007 SESS., at 74 (R.I. 2007), http://webserver.rilin.state.ri.us/Journals07/SenateJournals07/SJournal6-22.pdf (33 Yeas, 0 Nays); OKLA. STATE LEG., 2010 REG. SESS., HB2800 B. TRACKING REP. (2010), http://www.okhouse.gov/Journals/HJ2010/2010%20Hleg%20Day24.pdf (74 Ayes, 0 Nays); S.J. 46, 52ND LEG., 2D REG. SESS., at 1352 (Okla. 2010), http://www.oksenate.gov/publications/senate_journals/sj2010/sj20100421.pdf (46 Ayes, 0 Nays); S. JUDICIARY & RULES COMM., S.B. 1044 (Idaho 2011), https://legislature.idaho.gov/legislation/2011/S1044.htm (64 Ayes, 0 Nays (House); 34 Ayes, 0 Nays (Senate)); H.J. 48, 2014 REG. SESS., at 86-87 (La. 2014), http://house.louisiana.gov/H_Journals/H_Journals_All/2014_RSJournals/14RS%20-%20HJ%200530%2048.PDF (75 Yeas, 18 Nays); S.J. 45, 2014 REG. SESS., at 31-32 (La. 2014), http://senate.la.gov/sessioninfo/journals/2014/06-01-2014.pdf (38 Yeas, 0 Nays). The votes in Virginia and Nevada were similar. For information about the votes in those two states, *see* VA. LEG. INFO. SYS., HB 1752 S.: PASSED S. WITH SUBSTITUTION, 2013 SESS. (Va. 2013), http://lis.virginia.gov/cgi-bin/legp604.exe?131+vot+SV0637HB1752+HB1752 (40 Yeas, 0 Nays); VA. LEG. INFO. SYS., HB 1752 HOUSE: VOTE: PASSAGE, 2013 SESS. (Va. 2013), http://lis.virginia.gov/cgi-bin/legp604.exe?131+vot+HV1098+HB1752 (95 Yeas, 0 Nays)); NEV. LEG., 77TH SESS., VOTE ON SB131 (1ST REPRINT) ON S. FINAL PASSAGE (2013), http://www.leg.state.nv.us/Session/77th2013/Reports/BillVote.cfm?VoteID=274&fldReprint=1&fldDocTypeCode=SB&fldBillNumber=131&fldBillname=SB131 (20 Yeas, 0 Nays) NEV. LEG., 77TH SESS., VOTE ON SB131 (3D REPRINT) ON ASSEMB. FINAL PASSAGE (2013), http://www.leg.state.nv.us/Session/77th2013/Reports/BillVote.cfm?VoteID=1959&fldReprint=3&fldDocTypeCode=SB&fldBillNumber=131&fldBillname=SB131 (40 Yeas, 0 Nays).

96 *See* legislature votes cited *supra* note 95.

97 *See id.* These sums tally the votes cast in each branch of a state legislature that passed a post-mortem access statute. They exclude Virginia and Nevada because of the differences in those statutes compared to the other first and second generation statutes. *See supra* note 91. If the votes from Virginia and Nevada are included, the tally becomes 938 in favor and 18 against.

98 H.J. 48, 2014 REG. SESS., at 86-87 (La. 2014); S.J. 45, 2014 REG. SESS., at 31-32 (La. 2014).

99 *See, e.g.*, LEG. SERVS. AGENCY, OFFICE OF FISCAL & MGMT. ANALYSIS, 115TH GEN. ASSEMB., FISCAL IMPACT STATEMENT S.B. 212 (Ind. 2007), http://www.in.gov/legislative/bills/2007/PDF/

passed the first and second-generation statutes generally concluded that mandating post-mortem access to an online account had no fiscal impact on the state's budget.[100] Connecticut, for example, summarily found that "[t]he bill makes a minor change to the statutes involving the disclosure of certain information pursuant to the execution or administration of an estate. This change has no fiscal impact."[101] Finding that there is no financial effect on the state's budget does not mean that requiring post-mortem access is a cost-free transaction, but only that whatever costs are associated with the legislation will not be paid out of the state's bank account.[102] As a result, a final vote that is largely, if not unanimously, in favor of requiring access to a decedent's online accounts is predictable. In the absence of electoral consequences, the transfer of transaction costs coupled with the possible benefit for estate administration makes a legislator's decision to vote in favor of an access measure rather straightforward.

B. *Seeking Post-Mortem Access In and Out of the Courtroom*

Absent a state statute requiring default access or a list of accounts with associated passwords a personal representative encounters numerous obstacles when trying to settle the estate of a decedent who, like most people, lived a portion of his life online. While punishment for violating state privacy laws is a concern,[103] the basic problem confronted by a personal representative stems from terms of service agreements between a decedent and a service provider.[104] Some terms of service contain explicit clauses governing the transferability of an account at death while others leave the subject open to question. For example, Yahoo!'s terms of service declare that

> [y]ou agree that your Yahoo[!] account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt

---

FISCAL/SB0212.008.pdf; JANICE BUCHANAN, 52ND LEG. 2D SESS., BILL SUMMARY H.B. 2800 (Nev. 2010), http://webserver1.lsb.state.ok.us/CF/2009-10%20SUPPORT%20DOCUMENTS/BILLSUM/House/HB2800%20INT%20BILLSUM.doc; STATE OF IDAHO LEG., 2011 SESS., STATEMENT OF PURPOSE/FISCAL NOTE S.B. 1044 (2011), https://legislature.idaho.gov/legislation/2011/S1044SOP.pdf; LA. LEG. FISCAL OFFICE, 2014 REG. SESS., FISCAL NOTE S.B. 461 (2014), http://www.legis.la.gov/Legis/ViewDocument.aspx?d=916623.

100 *See* fiscal impact statements cited *supra* note 99.

101 OFFICE OF FISCAL ANALYSIS, SESS. YEAR 2005, FISCAL NOTE S.B. 262 (Conn. 2005).

102 *See id.*; *see also* fiscal impact statements cited *supra* note 99.

103 *See* Cahn et al., *supra* note 14, at 9.

104 *See id.* at 6.

> of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.[105]

But unlike Yahoo!'s clear description of what happens at the death of the user, Facebook's terms of service state that "[y]ou will not transfer your account . . . to anyone without first getting our written permission."[106] Facebook's provision unambiguously applies to inter vivos transfers, but leaves post-mortem availability in doubt.[107] Regardless of the clarity of the terms of service, personal representatives are often left to ask a service provider for access to a decedent's online account. Thus, a service provider may deny such a request for access in reliance on its own interpretation of the terms of service agreement.

Denials of post-mortem access to an online account that reference terms of service agreements have sent some personal representatives to the courthouse seeking a court order to compel access.[108] In many, perhaps most, of the instances where post-mortem access is sought, a loved one passes away, access to an online account is requested, the online service provider denies access, and a complaint is filed seeking compulsory disclosure of the account's contents. An early example of the tussle between an access seeker and an Internet service provider is the well-documented experience of Justin Ellsworth's family.[109] Following Justin's death in 2004 from injuries suffered while defusing a roadside bomb in Iraq,[110] Justin's father, John Ellsworth, sought access to his son's Yahoo! email account so that the family could learn more about Justin's life in Iraq.[111] However, John did not have the password to the account; therefore, he asked Yahoo! for access.[112] Yahoo! refused to provide access to Justin's account on that ground that doing so protected

---

105 *Yahoo Terms of Service*, YAHOO! § 28, https://policies.yahoo.com/us/en/yahoo/terms/utos/index.htm (last updated March 16, 2012).

106 *Statement of Rights and Responsibilities*, FACEBOOK § 4(9), https://www.facebook.com/legal/terms (last revised Jan. 30, 2015).

107 Stephanie Buck, *How 1 Billion People are Coping with Death and Facebook*, MASHABLE.COM (Feb. 13, 2013), http://mashable.com/2013/02/13/facebook-after-death/#36W5nIoOpiqV.

108 *See* Cahn et al., *supra* note 14, at 7.

109 The struggle to obtain Justin Ellsworth's emails has been discussed in numerous academic and practitioner journals. *See, e.g.*, Banta, *supra* note 34, at 833; Gerry W. Beyer & Naomi Cahn, *Digital Planning: The Future of Elder Law*, 9 NAELA J. 135, 148 (2013); Jason Mazzone, *Facebook's Afterlife*, 90 N.C. L. REV. 1643, 1664 (2012); Greg Lastowka & Trisha Hall, *Living and Dying in a Virtual World*, 284 N.J. LAW., Oct. 2013, at 29, 30.

110 Joel Thurtell & Cecil Angel, *Marine Dies Trying to Save Others*, DETROIT FREE PRESS (Nov. 16, 2004), http://www.justinellsworth.net/articles/detroit%20free%20press%20nov%2016.htm.

111 *Yahoo to Preserve E-Mail of Marine Killed in Iraq*, USA TODAY (March 1, 2005), http://usatoday30.usatoday.com/tech/news/2005-03-01-yahoo-email-save_x.htm. For a description of similar situations, *see, e.g.*, Ariana Eunjung Cha, *After Death, A Fight for Digital Memories: No Clear Laws of Inheritance Cover Web Data*, WASH. POST (Feb. 3, 2005), http://www.washingtonpost.com/wp-dyn/articles/A58836-2005Feb2.html.

112 *Yahoo to Preserve Email*, *supra* note 111.

the privacy of the account.[113] Furthermore, Yahoo!'s terms of service stated that an account terminates at death, and that an inactive account can be terminated after a period of inactivity.[114] With the clock running, John filed suit in a Michigan court seeking to compel Yahoo! to release the contents of Justin's email account.[115] The court ordered Yahoo! to transfer the contents of Justin's account, and Yahoo! voluntarily complied with the order.[116] Yahoo! delivered a CD to John Ellsworth containing 10,000 pages of material from Justin's account.[117] Despite receiving the information, the process of obtaining that information exacted an emotional toll on the Ellsworth family.[118]

Terms of service not only impede access for those without a password, but also for those who possess an account's password because of a decedent's planning or happenstance. After the death of her son in a motorcycle accident, Karen Williams sought access to his Facebook account, but did not have the account's password.[119] Williams contacted Facebook seeking access, but one of her son's friends provided "a tip" about the password that allowed her to discern the password and access the account.[120] According to Williams, "[i]t was like a gift."[121] Accessing her son's account, however, violated Facebook's terms of service regarding unauthorized access; therefore, Facebook changed the password to the account, thereby barring Williams' access.[122] Williams filed suit to access the account and prevailed, but only after a two-year legal battle.[123] Although successful in the courtroom, Williams only obtained access to the account for ten months, at which point Facebook terminated the account.[124] The legal victory fell short of the desired "full and

---

113 *Id.*

114 *The Abrams Report*, MSNBC (Dec. 21, 2004), http://www.justinellsworth.net/email/abrams%20rpt.htm (transcript of an MSNBC television broadcast discussing the ban on transfer as a barrier to disclosure).

115 Paul Sancya, *Yahoo Will Give Family Slain Marine's E-Mail Account*, USA TODAY (April 21, 2005), http://usatoday30.usatoday.com/tech/news/2005-04-21-marine-e-mail_x.htm.

116 *Id.*

117 Jennifer Chambers, *Family Gets GI's Email*, DETROIT NEWS (April 21, 2005), http://www.justinellsworth.net/email/detnewsapr.htm (also noting that the CD delivered by Yahoo did not contain any of the messages written by Justin. John Ellsworth thought that "maybe that's all [Justin] had." Yahoo was apparently attempting to "resolve the confusion over the CD").

118 *Id.* (describing the various emotions experienced throughout the process).

119 *In Death, Facebook Photos Could Fade Away Forever*, USA TODAY (March 1, 2013), http://www.usatoday.com/story/tech/2013/03/01/in-death-facebook-photos-could-fade-away-forever/1955933/.

120 *Id.*

121 *Id.*

122 *Id.* (describing the justification for termination as "company policy").

123 *Karen Williams' Facebook Saga Raises Questions of Whether User's Profiles Are Part of 'Digital Estates'*, HUFF POST: TECH (March 15, 2012), http://www.huffingtonpost.com/2012/03/15/karen-williams-facebook_n_1349128.html.

124 *Id.*

unobstructed access,"[125] but it represents more than a symbolic victory—Williams obtained access despite the terms of service, even if only for a limited amount of time.

Despite legal confrontations that have resulted in court-ordered access, published opinions offering insight into judicial views about disputes over access to online accounts are sparse. One exception to that scarcity is *Ajemian v. Yahoo!, Inc.*.[126] In *Ajemian*, the co-administrators of a decedent's estate requested information that was in decedent's Yahoo! email account, and Yahoo! agreed to provide header information associated with the account's emails, but not the content of those emails.[127] Later, and maybe predictably, the representatives sought a court order to compel disclosure of the content of the email messages on the ground that the email messages constituted property of the decedent.[128] Yahoo! challenged the request, relying upon several provisions of the terms of service governing civil procedure.[129] Contravening the property assertion of the complainants, Yahoo! argued that "emails in the account are not property of the estate."[130] Furthermore, Yahoo! claimed that revealing email content, even to an administrator of a decedent's estate, would violate the SCA.[131] The court decided the case on procedural grounds without reaching the merits of the property claim;[132] therefore, the question regarding ownership and access to the contents of the account went unresolved. Nevertheless, *Ajemian's* facts demonstrate that while estate representatives may obtain a catalogue of account information through negotiation, attempts to acquire account content may be resisted based upon terms of service agreements and federal privacy law.

Obstacles notwithstanding, estate representatives often gain access to an online account one way or another. Some, like Karen Williams, obtain account information by court order, while others, like the plaintiffs in *Ajemian*, secure information from an online account by negotiation. Whatever the route to relief, interested parties may not retrieve all of the desired

---

125 *Id.*

126 987 N.E.2d 604 (Mass. App. Ct. 2013).

127 *Id.* at 608–09. Yahoo! did not challenge the court order for header information. *Id.*

128 *Id.* at 609.

129 *Id.* (noting that Yahoo! argued that the terms of service provisions required that the suit be brought in California and contained a one-year statute of limitations rendering the suit untimely. Yahoo! also asserted that res judicata barred the claim.).

130 *Id.* at 610.

131 *Id.* at 609. Yahoo! asserted the SCA argument in a footnote. *Id.* at 615. Interestingly, one of the co-administrators of the decedent's estate opened the email account for the decedent, had "continued to access the account from time to time," but had "forgotten the password." *Id.* at 608. The co-administrators sought access on the basis of the co-ownership of one of the co-administrators in the second complaint. *Id.* at 609. Yet, Yahoo still refused to provide access to the account. *Id.* at 609–10.

132 *Ajemian*, 987 N.E.2d at 615–16 (basing the ruling on forum selection and limitations clauses in the terms of service agreement without deciding whether the contents of the emails were property of decedent's estate).

information from a decedent's online account. Like the short lived relief awarded to Karen Williams,[133] the 10,000 pages of material on the CD awarded to John Ellsworth did not contain any of the messages that his son had sent to others.[134] Similarly, the initial negotiations between Ajemian's representatives and Yahoo! resulted in a partial catalog of the account's contents—header information detailing the communicating parties and the date of the messages—but no content.[135] Court filings, time, and energy consuming negotiations may be just the first step of a long path toward the desired "full and unobstructed access" to a decedent's online accounts.[136]

On a fundamental level, the foregoing examples represent a tug-of-war between two basic principles—property rights versus the right to privacy. From the perspective of access seekers, the information in the online account is property owned by the account user to be distributed at the user's death. Karen Williams argued, for example, that "[i]f [the online account] w[as] a box of letters under his bed, no one would have thought twice."[137] On the other hand, online service providers are ceaselessly concerned with the privacy of their consumers in an age of hacking and phishing. Following the conclusion of the Ellsworth legal battle and the delivery of the CD, a representative for Yahoo! stated that it was "pleased the court has issued an order resolving this matter . . . and allowing Yahoo! to uphold our privacy commitment to our users."[138] In addition to the individual privacy settings available to its users,[139] Facebook's Data Policy states that "[w]e may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) *if we have a good faith belief that the law requires us to do so*."[140] From the perspective of the online service provider, whatever property rights a decedent may have in the contents of an account are trumped by the provider's commitment to the privacy interests of its users.

---

133 *See supra* note 123 and accompanying text.

134 *See* Chambers, *supra* note 117 (describing the CD as containing some "numerical gibberish." After being contacted by the family, Yahoo! claimed that it was "attempting to resolve the confusion over the CD").

135 *Ajemian*, 987 N.E.2d at 609.

136 *See* Chambers, *supra* note 123 and accompanying text.

137 *Mother Fights for Access to her Deceased Son's Facebook Account*, CBC NEWS (Mar. 1, 2013), http://www.cbc.ca/news/technology/mother-fights-for-access-to-her-deceased-son-s-facebook-account-1.1327683. *See also* Tom Hauser, *Family Fights to Access Late Son's Digital Data*, KTSP.COM (Jan. 21, 2015), https://web.archive.org/web/20150124034257/http://kstp.com/article/stories/s3682368.shtml ("'Imagine if your bank chose to treat your assets in the same way [that digital data is treated] . . . .'").

138 Chambers, *supra* note 117.

139 *See Facebook Privacy Basics*, FACEBOOK, https://www.facebook.com/about/basics (last visited Aug. 8, 2016).

140 *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Aug. 27, 2016) (emphasis added).

C. *Third Generation Uniform Statutes*

According to a study conducted by the Pew Research Center, only 7% of American adults used social networking sites at the time Connecticut enacted the first access statute in 2005.[141] By 2015, the percentage of American adults using such sites had rocketed to 65%.[142] Despite the proliferation of the online world and media coverage of disputes between access seekers and service providers, a mere nine states had enacted access statutes by the end of 2014.[143] The absence of statutory guidance not only created legal uncertainty in states without a statute, but also risked waste given the potential value of data stored in online accounts. And to the extent statutory law existed in 2014, statutes differed in the types of accounts that could be accessed by a personal representative as well as the authority granted to a personal representative to handle account information.[144] While Connecticut requires an online service provider to provide "access to or copies of the contents of" a decedent's email account,[145] Oklahoma authorizes personal representatives to access a wide variety of digital accounts and permits an array of actions to be taken regarding those accounts, including termination.[146] Furthermore, ambiguity in terms of service agreements regarding the status of an account following a user's death, as well as uncertainty about liability under state or federal privacy laws, only added to the challenges faced by personal representatives during estate administration.[147] In short, unpredictability pervaded the issue of post-mortem access to digital assets.

The muddled legal landscape and the probable increase of access problems in the future prompted the Uniform Law Commission to address the problem of post-mortem access to online accounts in 2011.[148] After a three-year drafting process, the ULC introduced the first of the third generation statutes in 2014, the Uniform Access to Digital Assets Act.[149] The first sentence of UFADAA declares that "[t]he purpose of this Act is to vest fiduci-

---

141 Andrew Perrin, *Social Media Usage: 2005-2015*, PEW RES. CTR. (Oct. 8, 2015), http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.

142 *Id.*

143 *See* Alexandra Elliott, Comment, *Death and Social Media Implications for the Young and Willless*, 55 JURIMETRICS J. 381, 394–96 (2015). The states are: Connecticut (2005), Delaware (2014), Indiana (2007), Rhode Island (2007), Oklahoma (2010), Idaho (2011), Virginia (2011), Nevada (2013), and Louisiana (2014).

144 *See supra* notes 81–91 and accompanying text.

145 CONN. GEN. STAT. ANN. § 45a-334a(b) (West 2015).

146 OKLA. STAT. ANN. tit. 58, § 269 (West 2016).

147 *See* Elliott, *supra* note 143, at 396–97.

148 *See* Hennig Letter, *supra* note 41.

149 UFADAA, *supra* note 44.

aries with the authority to access, control, or copy digital assets and accounts."[150] Functionally, UFADAA sought to "remove barriers to a fiduciary's access to electronic records" in the form of disparate access laws, terms of service agreements, and privacy protections under state and federal law.[151] Given the dissimilar treatment of the issue under the paucity of existing laws, the ULC concluded "[a] uniform approach among states will provide certainty and predictability for courts, account holders, fiduciaries, and Internet service providers."[152]

One of the primary challenges faced by UFADAA's drafters was how to define a "digital asset" to be accessed upon proof of death of an account holder. First and second-generation access statutes explicitly identified the types of online accounts accessible by personal representatives. Connecticut's statute permitted access to email accounts only while Idaho's law listed everything from an email account to a microblog as being accessible to an estate representative.[153] The problem with that approach is that identifying the type of account with such specificity makes the statute insensitive to technological change. For example, two of today's most popular sites, Twitter and Instagram, did not exist when Connecticut decided to grant personal representatives access to email accounts only.[154] As technology advances, a positive feedback cycle develops: digital innovation attracts users and the increased number of users spurs developers to innovate. As the cycle continues, however, laws governing post-mortem access to digital assets remain frozen on the books and eventually become outmoded.

To avoid the specification pitfall of existing statutes, comments offered during UFADAA's drafting process stressed the importance of crafting provisions that would allow the law to keep pace with technological changes without subsequent amendment.[155] With that in mind, section two of UFADAA broadly, and succinctly, defined "digital asset" to mean "a record that is electronic."[156] Parsing the definition of "digital asset" more finely,

---

150 *Id.* at 1 (Prefatory Note).

151 *Id.*

152 *Id.*

153 *Compare* 2005 Conn. Pub. Acts 05-136, https://www.cga.ct.gov/2005/ACT/PA/2005PA-00136-R00SB-00262-PA.htm; *with* IDAHO CODE § 15-3-715 (2015), https://legislature.idaho.gov/idstat/Title15/T15CH3SECT15-3-715.htm.

154 *See* Gerry Shih & Alexei Oreskovic, *How Little 'Twitter' Became a Magnificent Money Machine*, BUSINESS INSIDER (Sept. 17, 2013), http://www.businessinsider.com/history-of-twitter-2013-9 (Twitter); *Instagram: A Brief History*, SFGATE (Dec. 18, 2012, 10:06 PM), http://www.sfgate.com/technology/article/Instagram-a-brief-history-4129827.php (Instagram).

155 Memorandum from Chris Kunz to Suzy Walsh and Naomi Cahn (Mar. 17, 2014), http://www.uniformlaws.org./Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets; Letter from John Gregory and Chris Kunz to Suzy Walsh and Naomi Cahn (Feb. 23, 2014), http://www.uniformlaws.org./Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets;

156 *See* UFADAA, *supra* note 44, § 2.

UFADAA defines "record" to mean "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[157] Furthermore, "electronic" means "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities."[158] Unlike the limited scope of coverage under first-generation statutes and the specific enumerations of accounts in second-generation statutes, UFADAA's definitions offer flexibility to cover whatever online innovation captures the market in the future.

For personal representatives and survivors of the decedent, UFADAA's most important provision is section four, which eliminates the barriers to access plaguing estate administration.[159] Under section four, personal representatives have a "right" to access "the content of an electronic communication" maintained by an online service provider unless such access is barred by the decedent's will or prohibited by the Electronic Communications Privacy Act (ECPA).[160] The ECPA permits disclosure of the content of communications received by an individual to that individual or an agent of that individual or a third party with the "lawful consent" of the recipient of the message.[161] However, communications created by the account holder are not available to third parties, like personal representatives, without the "lawful consent" of the drafter.[162] In other words, a personal representative may access the content of emails received by the decedent, but would need the "lawful consent" of the decedent to access the content of messages sent by the decedent.[163] Furthermore, section four authorizes a personal representative to access a catalogue (not the content) of messages "sent or received" by the decedent as well as "any other digital asset in which at death the decedent had a right or interest."[164] In conjunction with the definition of "digital asset," UFADAA § 4 vanquishes uncertainty about access to a decedent's online accounts by establishing a default rule of access unless prohibited by a provision in the decedent's will or federal law.[165]

While it may be the most useful for parties interested in access, section four also proved to be UFADAA's most controversial provision. During the drafting process, a number of parties voiced concerns about breaching the

---

157 *Id.*

158 *Id.*

159 *Id.* § 4.

160 *Id.* "Content of an electronic communication" is defined as "information concerning the substance or meaning of the communication which: (A) has been sent or received by an account holder; (B) is in electronic storage by a custodian providing an electronic-communication service to the public or is carried or maintained by a custodian providing a remote-computing service to the public; and (C) is not readily accessible to the public." *Id.* § 2(6).

161 *Id.* § 4 cmt.

162 UFADAA, *supra* note 44, § 4 cmt.

163 *Id.*

164 *Id.* §§ 4(2), 4(3).

165 *Id.* § 4.

privacy of persons who had sent communications to a decedent that remained in the decedent's account at death.[166] The ACLU, for example, asserted that providing "nearly unfettered access to online accounts or online content" risked violating the privacy of both senders and recipients of online communications.[167] Furthermore, the ACLU noted that some accounts lacked "offline equivalents," such as a profile on an Internet dating site, and that providing ready access to that material encroached upon the privacy of the deceased account holder.[168] Tying UFADAA's default rule permitting access to federal privacy law, NetChoice argued that "[t]he contents of subscriber communications may not even be disclosed by an Internet company in response to judicial process in civil litigation" under the ECPA.[169] If an online service provider disclosed the contents of an email held in a decedent's account, the sender of the email could file suit against the disclosing service provider and receive statutory damages and attorney's fees to remedy the ECPA violation.[170] Although the ULC anticipated privacy-related criticism and sought to forestall it by providing two draft versions of section four,[171] the final version granted access to personal representatives by default.[172]

For UFADAA's critics, the ULC's drafting process represented only the first round in the battle, as an uniform act requires state legislative action to become law. After completing its work, the ULC promulgated UFADAA and the effort proved successful in terms of introduction to state legislatures—twenty-six states placed UFADAA bills on their agendas during their legislative sessions.[173] States from Massachusetts to Hawaii, which had failed to enact either first or second-generation statutes, appeared ready to provide personal representatives with access to a decedent's digital assets.[174] Given the voting totals associated with the passage of first and second-generation statutes, one might have predicted that UFADAA's swift introduction into a majority of state legislatures would mean that enactment was largely perfunctory. However, all but one of the UFADAA bills died before a vote had

166 *See* Bohm letter, *supra* note 43; DelBianco et al. Letter, *supra* note 43.

167 *See* Bohm Letter, *supra* note 43.

168 *Id.*

169 *See* DelBianco et al. Letter, *supra* note 43.

170 *Id.*

171 FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 4 (UNIF. LAW COMM'N, Draft 2013), http://www.uniformlaws.org./Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets (containing two alternatives for § 4). According to the Comment for § 4, Alternative A "responds to the concerns of internet service providers who believe that the act should be structured to clarify the difference between fiduciary authority over digital property other than electronic communications protected by federal law (the Electronic Communications Privacy Act (ECPA)), and authority over ECPA-covered electronic communications." *Id.* § 4 cmt. Alternative B establishes the default rule that the personal representative is authorized to administer all of the decedent's digital property, regardless of whether it is covered by ECPA." *Id.* § 4 Alternative B.

172 UFADAA, *supra* note 58, at § 4.

173 *See Legislation*, UNIF. LAW COMM'N, *supra* note 46.

174 *Id.*

been taken.[175] Only Delaware enacted a post-mortem access bill based upon UFADAA—and it did so "before the opposition was organized."[176]

The basic reason that UFADAA imploded in state legislative halls centers on the privacy-related concerns identified during the ULC's drafting process. The Senior Legal Director at Yahoo!, for example, blogged that UFADAA did "not ensure the privacy of sensitive or confidential information shared by the decedent or third parties."[177] Yahoo! further claimed that UFADAA was based upon "the faulty presumption that the decedent would have wanted the trustee to have access to his or her communications."[178] Even after Delaware's legislature passed a UFADAA bill, Google, AOL, NetChoice, and others urged Delaware's governor to veto the bill because it eliminated privacy protections for citizens of Delaware, forced service providers to risk violations of state or federal law, and ignored terms of service agreements between Delawareans and service providers.[179] Similarly, advocacy groups like the Electronic Frontier Foundation and Consumer Action lined up against UFADAA based upon privacy and autonomy concerns.[180] In fact, these groups sent a joint letter in opposition to UFADAA to each state legislature considering a UFADAA bill.[181] Although the opposition lost the fight in Delaware, opponents might justifiably conclude that they won the legislative war given UFADAA's defeat in every other state where the Act was considered.[182]

In addition to conducting an anti-UFADAA campaign, UFADAA's critics drafted an alternative statute to compete with UFADAA. The stated purpose of the Privacy Expectation Afterlife Choices Act ("PEAC") is "to pro-

---

175 *Id.*

176 *Id.*; Letter from Benjamin Oreske, Legislative Counsel, Unif. Law Comm'n, to Senator Stewart J. Greenleaf, Chairman, Pa. Senate Judiciary Comm. (June 15, 2015), http://judiciary.pasenategop.com/files/2015/06/Uniform-Law-Commission-Written-Testimony.pdf.

177 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.

178 *Id.*

179 Zach Miners, *Yahoo Slams New "Digital Will" Law, Says Users Have Privacy When They Die*, PCWORLD (Sept. 15, 2014), http://www.pcworld.com/article/2683472/yahoo-slams-new-digital-will-law-says-users-have-privacy-when-they-die.html (containing a link to the letter written to Delaware's governor).

180 Letter from Daniel M. Gluck, Legal Dir., Am. Civil Liberties Union of Haw. to Chair McKelvey and Members of the Comm. on Consumer Prot. and Com. (Feb. 4, 2015), http://www.capitol.hawaii.gov/Session2015/Testimony/HB745_TESTIMONY_CPC_02-04-15_.PDF.

181 Benjamin Feist, 2015 *Legislative Session Wrap-Up*, AM. CIV. L. UNION OF MINN. (2015), https://www.aclu-mn.org/files/2714/3655/4439/2015_Legislative_Report.pdf ("The National ACLU and other civil liberties organizations sent a letter in opposition to UFADAA to each state legislature where the issue was introduced, including Minnesota."). Minnesota's UFADAA bill was tabled without a vote. *Id.*

182 *See Legislation*, UNIF. LAW COMM'N, *supra* note 46.

tect[] a decedent's private communications . . . while facilitating administration of a decedent's estate."[183] To fulfill its purpose, PEAC differentiates access requirements by the type of account information being sought by the personal representative.[184] A personal representative may receive a copy of a record/catalogue of communications (the "to" and "from" lines in an email) stored in the account directly from the online service provider.[185] Additionally, a personal representative may seek disclosure of the contents of the account.[186] The "contents" of the account include "any information concerning the substance, purport, or meaning of that communication."[187] If the request for access to account contents were approved, the personal representative would obtain far more information than that offered by a record of account contacts, as the personal representative would receive the substance of messages that were password-protected during the account holder's life.

As between the two classifications of accessible information available—a catalogue of correspondents and the contents of the account—the former is likely to be more important to the process of estate administration. Because personal representatives may have difficulty identifying financial accounts, a catalogue of account contacts "help[s] fiduciaries identify important interactions, like those with a bank or online broker, and then contact those institutions as part of closing the account."[188] Beyond institutional identities, a list of individuals who communicated with the decedent may reveal the identities of creditors that need to be paid, debts owed to the decedent, or unknown assets that need to be collected. In short, a catalogue of the communications sent and received by the decedent help a personal representative fulfill her fiduciary duties in an increasingly paperless world.

Substantively, PEAC requires a personal representative to go to court to obtain an order for disclosure regardless of the type of account information sought. To receive a record of account communications from an online service provider, PEAC section 1(A) declares that a personal representative must obtain a court order that includes findings that:

> (a) the user is deceased;
> (b) the deceased user was the subscriber to or customer of the provider;
> (c) the account(s) belonging to the deceased user have been identified with specificity, including a unique identifier assigned by the provider;

---

183 PEAC, *supra* note 54.

184 *Id.* at § 6.

185 *Id.* The PEAC defines a "record" of communication as having the same meaning employed by 18 U.S.C. § 2702 of the Stored Wire and Electronic Communications and Transactional Records Access Act, which identifies exceptions for disclosure of customer records. *See* 18 U.S.C. § 2702(c) (2015). *See also* NetChoice Two-Pager, *supra* note 62.

186 PEAC, *supra* note 54, § 1.

187 *See id.* § 6(A). For more on the distinction between a record and contents, see Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009).

188 NetChoice Two-Pager, *supra* note 62.

> (d) there are no other authorized users or owners of the deceased user's account(s);
> (e) disclosure is not in violation of 18 U.S.C. § 2701 *et seq.*, 47 U.S.C. § 222, or other applicable law;
> (f) the request for disclosure is narrowly tailored to effect the purpose of the administration of the estate,
> (g) the executor or administrator demonstrates a good faith belief that account records are relevant to resolve fiscal assets of the estate;
> (h) the request seeks information spanning no more than a year prior to the date of death; and
> (i) the request is not in conflict with the deceased user's will or testament.[189]

Obtaining a record of account contacts is likely to be most useful for personal representatives during estate administration, but the content of information held in online accounts is frequently the information most desired by those who survive the decedent. Survivors seek content information as a way to remember a loved one or in an attempt to understand what was happening in an individual's life just before death. Justin Ellsworth's father, for example, doggedly pursued access to his son's Facebook account to gather information for a scrapbook that he and his son had planned to create.[190] Similarly, Bill and Kristi Anderson sought access to their son's digital assets to search for clues that might help explain their son's "accidental" death.[191] For individuals in similar situations, estate administration is not about property, but about a person. As a result, the value of an account's contents far exceeds the value added by learning the "To" and "From" information disclosed by a catalogue of account contacts.

To obtain the contents of an account, PEAC's section 1(B) requires a personal representative to present an online service provider with "all of the following:"[192]

> (a) A written request for the contents of deceased user's account;
> (b) A copy of the death certificate of the deceased user; and
> (c) An order of the court of probate that by law has jurisdiction of the estate of a deceased user:
>
> > (i) finding that the will of the decedent or setting within the product or service regarding how the user's contents can be treated after a set period of inactivity or other event expressly consented to the disclosure of the contents of the deceased user's account by the executor or administrator of the estate of the deceased user;

---

189 PEAC, *supra* note 54, § 1. For a more detailed discussion of the relevant factors *see infra* notes 192–197 and accompanying text.

190 *See Yahoo to Preserve E-Mail*, *supra* note 111 (reporting that Justin and his father had discussed creating a scrapbook to contain Justin's emails).

191 Hauser, *supra* note 137; *see also* Emily Anne Epstein, *Family Fights to Access Son's Facebook Account After His Suicide to Finally Gain Closure Over Tragic Death*, DAILY MAIL (June 1, 2012), http://www.dailymail.co.uk/news/article-2153548/Family-fights-access-sons-Facebook-Gmail-accounts-suicide.html.

192 PEAC, *supra* note 54, § 1(B).

> (ii) ordering that the estate shall first indemnify the provider from all liability in complying with the order;
> (iii) finding that the user is deceased;
> (iv) finding that the deceased user was the subscriber to or customer of the provider;
> (v) finding that the account(s) belonging to the deceased user have been identified with specificity, including a unique identifier assigned by the provider;
> (vi) finding that there are no other authorized users or owners of the deceased user's account(s); and
> (vii) finding that disclosure of the contents is not in violation of 18 U.S.C. § 2701 *et seq.*, 47 U.S.C. § 222, or other applicable law.[193]

A comparison of the terms of UFADAA and PEAC demonstrates that the two legislative proposals reside at opposite ends of the privacy spectrum. UFADAA granted personal representatives access to an account's record and contents by default.[194] PEAC, however, discards default access in its entirety and requires a court order that makes multiple findings prior to disclosure of any account information.[195] Furthermore, even if a personal representative obtains the necessary court order for disclosure of a record of communications or account contents under PEAC, a possibility exists that a record or contents of the account will remain out of reach.[196] PEAC's section two requires a court to quash the order "if compliance with such order otherwise would cause an undue burden on such provider."[197] As a result, the possibility exists that a court could issue an order for disclosure, an online service provider could delay complying with the order for a lengthy period of time, and then the online service provider could file a motion to quash the disclosure order.[198] In theory, the motion to quash could be filed after an estate is closed, which may require the re-opening of an estate if, for example, a debt is discovered in the online information.[199] Compared to UFADAA, PEAC erects numerous hurdles to overcome for personal representatives seeking access to any information in a decedent's online accounts; PEAC's default privacy setting is zero.

---

193 *Id.*

194 UFADAA, *supra* note 44, § 7.

195 *See* PEAC, *supra* note 54, § 1.

196 *Id.* at § 2.

197 *Id.*

198 Karin Prangley, *War and PEAC in Digital Assets: The Providers' PEAC Act Wages War with UFADAA*, PROB. & PROP., July-Aug. 2015, at 40, 44 ("[T]he PEAC Act allows a service provider to quash an order requiring disclosure or to refuse disclosure, even after the necessary court order has been obtained. The PEAC Act does not limit the amount of time that the provider may take to quash the order or refuse to disclose. At any time after the order has been issued, the provider could simply move to have the order quashed.").

199 *Id.* ("The PEAC Act also does not preclude the provider from moving to quash the order, even if the estate has been closed, and may necessitate the re-opening of estates that have been previously closed.").

Like UFADAA, PEAC became the subject of critical examination following its introduction to state legislatures.[200] One of the primary critiques of PEAC is that its mandate requiring separate court orders to access a record and content, respectively, slows the process of administering an estate.[201] A California Assembly member, for example, placed a PEAC bill on the legislative agenda in early 2015.[202] As part of the normal legislative process, the state judiciary committee analyzed PEAC and opined that PEAC's mandate for court-ordered disclosure would "delay the estate administration and require the expenditure of estate assets in order to comply."[203] More specifically, the committee pointed out that a personal representative is legally required to file an inventory of the decedent's estate four months after the decedent's death and PEAC's requirements establish "a complex procedure" that increases the difficulty of meeting the inventory deadline.[204] Given the number and complexity of court adjudications, complying with PEAC's provisions risked a "delay distribution of estate assets or payments to heirs or creditors."[205]

PEAC not only differed from UFADAA on the core issue of default access to digital assets, but also in the important category of scorekeeping.[206] Unlike UFADAA's widespread consideration in state legislatures across the nation, a mere four states contemplated PEAC bills during their 2015 legislative sessions.[207] California halted consideration of its PEAC bill during the last quarter of 2015.[208] Oregon has held public hearings on its PEAC bill,

---

200 For an overview of possible objections to PEAC *see id.* at 41–44.

201 *E.g.*, CAL. S. JUDICIARY COMM., REPORT ON THE PRIVACY EXPECTATION AFTERLIFE AND CHOICES ACT, Assemb. B. 691 (Calderon) (July 13, 2015), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160AB691 (click on "07/13/15- Senate Judiciary").

202 Bill History, Assemb. B. 691, 2015-2016 Leg. Sess. (Cal. 2016), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB691 (click on "History") [hereinafter Cal. Bill History].

203 CAL. S. JUDICIARY COMM., *supra* note 201.

204 *Id.* at 18–19.

205 *Id.* at 19.

206 In addition, PEAC is narrower in scope because it addresses only access/disclosure as it relates to personal representatives of decedents' estates. UFADAA and RUFADAA comprehend access/disclosure to fiduciaries as a general matter. *Compare* UFADAA, *supra* note 44 § 3(a) *and* RUFADAA, *supra* note 58 at § 3(a), *with* PEAC, *supra* note 54 § 1(B).

207 *See* Cal. Bill History, *supra* note 202; History S.B. 1450, 2015 Sess. (Va. 2015), http://lis.virginia.gov/151/sum/SB1450.HTM [hereinafter Va. Bill History]; *Wyoming Privacy Expectation Afterlife and Choices Act* (Working Draft 16 LSO-0041, Wyo. 2016), http://legisweb.state.wy.us/interimCommittee/2015/16LSO-0041-0.5.pdf [Wyoming Draft Bill]; Overview, H.B. 2647, 78th Or. Leg. Assemb., Reg. Sess. (Or. 2015), https://olis.leg.state.or.us/liz/2015R1/Measures/Overview/HB2647 (click on "Measure History") [hereinafter Oregon Bill Overview].

208 *See* Cal. Bill History, *supra* note 202.

which remains in committee,[209] and, unsurprisingly, the ACLU offered testimony in support of passage.[210] Similarly, Wyoming's Task For on Digital Information Privacy is studying PEAC in advance of a possible vote in 2016.[211] At present, Virginia is the only state to pass PEAC, which became part of the Virginia Code in mid-2015.[212]

While NetChoice drafted PEAC, the ULC returned to the drawing board in acknowledgement of the privacy criticisms aimed at UFADAA, and produced a revised version of UFADAA (RUFADAA) almost one year later.[213] According to a 2015 memorandum from the ULC's annual meeting, UFADAA's opponents "participated in the drafting process, [but] they did not articulate or engage in serious discussions about their concerns until recently."[214] The ULC asserted that "[t]he proposed amendments, although extensive in form, will not substantially change the purpose or effect of the act."[215] Despite the changes, the ULC intended the revisions to retain the access and disclosure authority granted to personal representatives under UFADAA.[216] In the end, the ULC hoped that the changes would "serve the essential purposes of the act and substantially decrease opposition to its enactment."[217]

For the purposes of estate administration, the most important provision under RUFADAA is section eight and its requirements to obtain a catalogue of communications stored in a decedent's account.[218] Section eight of RUFADAA requires the service provider to transfer a catalogue of the communications stored in the account to the personal representative unless prohibited by the user or a court.[219] To trigger disclosure of an account catalogue, a personal representative must proffer a written request for a catalogue, a copy of the decedent's death certificate, and letters testamentary to the online

---

209 Oregon Bill Overview, *supra* note 206.

210 *Hearing on H.B. 2647 Before the H. Comm. on the Judiciary, 2015 Sess.* (Or. 2015) (testimony of Kimberly McCullough, Legislative Dir., Am. Civ. Liberty Union of Or.), https://olis.leg.state.or.us/liz/2015R1/Downloads/CommitteeMeetingDocument/53223.

211 Wyoming Draft Bill, *supra* note 207.

212 VA. CODE ANN. § 64.2-109 (2015); see also Va. Bill History, supra note 207.

213 RUFADAA, *supra* note 58. The revised version remains broader than PEAC by covering various types of fiduciaries in addition to personal representatives of a decedent's estate.

214 Memorandum from the Unif. Law Comm'n (Dec. 7, 2007), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/UFADAA_Explanation%20of%20proposed%20amendments_2015AM.pdf [hereinafter RUFADAA Memo].

215 *Id.*

216 *Id.*

217 *Id.*

218 RUFADAA defines a "catalogue of electronic communications" as "information that identifies each person with which a user has had an electronic communication, the time and date of the communication, and the electronic address of the person." RUFADAA, *supra* note 58, § 2(4).

219 *Id.* § 8.

service provider.[220] Furthermore, RUFADAA requires a personal representative to provide the following "if requested by the custodian" of the account:

> (A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;
> (B) evidence linking the account to the user;
> (C) an affidavit stating that the disclosure of the user's digital assets is reasonably necessary for estate administration; or
> (D) a finding by the court that:
> (i) the user had a specific account with the custodian, identifiable by the information specified in subparagraph (A); or
> (ii) disclosure of the user's digital assets is reasonably necessary for estate administration.[221]

For a decedent's survivors interested in acquiring information about a decedent, RUFADAA's most important provision is section seven and its requirements for disclosure of account contents.[222] Section seven permits an online service provider to disclose the contents of a decedent's account "[i]f the user consented to disclosure or if a court orders disclosure."[223] In addition to evidence of a decedent's consent, the personal representative must provide the custodian with "a written request for disclosure in physical or electronic form," a copy of a death certificate, a copy of an instrument granting authority to act on behalf of the decedent, and a copy of the account holder's will.[224] Furthermore, the personal representative must, "if requested," provide

> (A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;
> (B) evidence linking the account to the user; or
> (C) a finding by the court that:
> (i) the user had a specific account with the custodian, identifiable by the information specified in subparagraph (A);
> (ii) disclosure of the content of electronic communications of the user would not violate 18 U.S.C. Section 2701 *et seq.* [as amended], 47 U.S.C. Section 222 [as amended], or other applicable law;
> (iii) unless the user provided direction using an online tool, the user consented to disclosure of the content of electronic communications; or
> (iv) disclosure of the content of electronoic communications of the user is reasonably necessary for administration of the estate.[225]

---

220 *Id.*

221 *Id.*

222 RUFADAA defines the "content" of an account as "information concerning the substance or meaning of the communication" that "has been sent or received by a user," is both "in electronic storage," and is "not readily accessible to the public." RUFADAA, *supra* note 58, § 2(6).

223 *Id.* § 7 cmt.

224 *Id.* § 7(1)–(4).

225 *Id.* §7(5).

The structural and substantive changes from UFADAA to RUFADAA reflect the effectiveness of the anti-UFADAA campaign. Structurally, RUFADAA discards UFADAA's single set of requirements for access to all account information, both record and contents, in favor of PEAC's bifurcated requirements to access a record of account communications and the contents of those communications.[226] Substantively, RUFADAA's privacy setting for an account record is similar to UFADAA's presumption of disclosure. Like UFADAA, RUFADAA requires an online service provider to deliver a record of account communications "unless the user prohibited disclosure of digital assets or the court directs otherwise."[227]

However, RUFADAA diverges from UFADAA by prohibiting disclosure of contents unless "the user consented to disclosure of the contents of electronic communications."[228] Further severing ties to its ancestor, RUFADAA declares that an online service provider may request a court order prior to disclosure of either a catalogue or contents.[229] By comparison, RUFADAA's presumption regarding disclosure of contents is more closely related to PEAC's presumption of nondisclosure than UFADAA's disclosure by default without court involvement. Because the revisions were "extensive in form," RUFADAA is, more or less, an entirely new model act;[230] and the new model act incorporates many of PEAC's privacy benchmarks.

Interestingly, NetChoice endorsed the ULC's revisions in early 2016, despite RUFADAA's textually permissive approach to the requirement of a court order for a record or contents of a digital account. According to a memorandum explaining its support, NetChoice described RUFADAA as a "privacy-centric" model that balanced the needs of fiduciaries and the privacy interests of account holders/correspondents while complying with federal law.[231] The language used in the memo, however, may foreshadow how RUFADAA is likely to function—at least from NetChoice's point of view. According to the memo, "[t]he probate court can order copies of the records of the communications for the fiduciary."[232] The terms of RUFADAA, however, permit an online service provider to provide a catalogue or contents without a court order; a court order is only required "if requested" by the service provider.[233] Similarly, NetChoice asserts that RUFADAA permits a personal representative to access the contents of digital accounts "*only* when the deceased expressly allowed it in their will or through user choice controls.

---

226 *Id.*

227 RUFADAA, *supra* note 58, § 8.

228 *Id.* § 7.

229 *Compare* RUFADAA, *supra* note 58, § 7(5), § 8(4), *with* UFADAA, *supra* note 44, § 4.

230 RUFADAA Memo, *supra* note 214.

231 NetChoice Two-Pager, *supra* note 62.

232 *Id.* In fairness, using the word "can" may also be interpreted to mean "may" and therefore reflect the terms of the model act as written.

233 RUFADAA, *supra* note 58, § 7(5) and § 8(4).

. . . subject to verification and indemnification processes."[234] The phrase "verification and indemnification processes" is vague and could refer to the court orders that an online service provider *may* request as part of the disclosure procedure.[235] NetChoice's PEAC is "privacy-centric" and mandates court involvement;[236] therefore, the probability that it would embrace RUFADAA's regulatory strategy if it impaired the interests of its members probably approaches zero.

Regardless of which third-generation statute is more widely embraced, the arguments made on the floors of state legislatures reflect those made by parties seeking judicially compelled post-mortem access to digital assets in states without positive law on the issue.[237] Access seekers like John Ellsworth and the plaintiffs in *Ajemian* based claims for access in court on the ground that the contents of the account belonged to deceased account users.[238] Parties opposing access in court asserted that denying access protected the privacy interests of those who communicated with the decedent.[239] On the legislative front, the Prefatory Note to UFADAA declares that it "promotes the fiduciary's ability to administer the account holder's property."[240] On the other hand, UFADAA's opponents decried the grant of access by default under its provisions and laud the privacy protections offered by PEAC and RUFADAA.[241] In effect, the tug-of-war over post-mortem access to digital assets has shifted from the courtroom to the legislature and the winner is yet to be determined.

II. ISOLATING POSTHUMOUS PRIVACY

Proponents and opponents of post-mortem access legislation generally agree about one basic principle—digital assets are property. The fiduciary friendly provisions of the now superseded UFADAA stated that one of its goals was to facilitate a personal representative's "ability to administer the account holder's property."[242] While generally opposed to unfettered post-mortem access, Google's terms of service declare that users "retain ownership of any intellectual property rights" in account content and, more simply

---

234 *See* NetChoice Two-Pager, *supra* note 62.

235 *Compare id.*, *with* RUFADAA, *supra* note 58, §§ 7(5), 8(4).

236 *See generally* PEAC, *supra* note 54.

237 *See supra* notes 194–199 and accompanying text (explaining that UFADAA and PEAC are on opposite sides of the privacy spectrum).

238 *See* Ajemian v. Yahoo!, Inc., 987 N.E.2d 604 (Mass. App. Ct. 2013); Abrams *supra* note 114.

239 *See* Abrams *supra* note 114 (discussing Ajemian, 987 N.E.2d 604).

240 UFADAA, *supra* note 44, at 2 (Prefatory Note). The online version of RUFADAA does not have a Prefatory Note.

241 *See supra* note 47–62 and accompanying text.

242 UFADAA, *supra* note 44 at 2 (Prefatory Note). Presumably, RUFADAA would serve the same purpose even though it does not have a Prefatory Note.

put, "what belongs to you stays yours."[243] Such statements in an online service provider's terms of service make it difficult to argue that the contents of an online account are not 'property'. Beyond legislators and lobbyists, the view that digital information is property of one sort or another predominates. The Internal Revenue Service even treats "virtual currency" as property for federal tax purposes; therefore, Bitcoin is subject to taxation.[244] Given the overwhelming view that digital assets are property, groups seeking to draft a rule to govern post-mortem access to digital assets do not press the argument that digital assets somehow fall outside the definition of "property."[245]

The general agreement about the status of digital assets as property, however, leaves room for debate about the privacy rights associated with a decedent's digital assets. For some, the issue of privacy does not present much of an obstacle to accessing information stored in a password-protected account. An article in an American Bar Association journal, *Probate & Property*, argued that "[t]his is not a privacy issue" because the protection offered by existing fiduciary law would impose liability if the fiduciary "went rogue with on-line access" or "broadcast the information to the world."[246] According to others, privacy advocates overlook the interests of families who might lose "all proof of existence of the decedent" or their existence "without some type of access" so "[g]aining a copy of all transmissions may not go far enough."[247] In short, the importance of fiduciary effectiveness coupled with

---

243 *Google Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms/ (last modified Apr. 14, 2014). *See also Statement of Rights and Responsibilities*, FACEBOOK, *supra* note 106.

244 I.R.S. Notice 2014-21, I.R.B. 2014-16 (Apr. 14, 2014). Furthermore, some jurisdictions recognize a claim for conversion of digital assets, which represents an acknowledgment that digital assets are "property." *See* RESTATEMENT (SECOND) OF TORTS § 222A (1965) (noting that conversion requires interference with "the right of another to control . . . the chattel."). For cases that recognize a claim for conversion of digital assets, *see, e.g.*, Kremen v. Cohen, 337 F.3d 1024, 1036 (9th Cir. 2003); Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1273 (N.Y. 2007). For more on New York's perspective, see David P. Miranda, *Doctrine of Conversion Applies to Electronic Property*, N.Y. ST. BAR ASS'N J., Feb. 2008, at 47. Massachusetts, on the other hand, does not recognize conversion of digital assets, *see In re* TJX Companies Retail Sec. Breach Litig., 527 F. Supp. 2d 209, 212–13 (D. Mass. 2007), *aff'd in part*, 564 F.3d 489 (1st Cir. 2009). For general discussion on conversion of digital assets, see Caitlin J. Akins, *Conversion of Digital Property: Protecting Consumers in the Age of Technology*, 23 LOY. CONSUMER L. REV. 215 (2010).

245 In addition, the failure to argue against property rights in account content avoids the thorny issue associated with intellectual property rights in the content of a digital account. For an example of the complications associated with labeling the content of an email account as "property," see Jonathan J. Darrow and Gerald R. Ferrera, *Who Owns a Decedent's Emails: Inheritable Probate Assets or Property of the Network?*, 10 N.Y.U. J. LEGIS. & PUB. POL'Y 281 (2006).

246 Victoria Blachly, *Uniform Fiduciary Access to Digital Assets Act: What UFADAA Know*, 29 PROB. & PROP., July-Aug. 2015, at 8, 19. *See also* Benjamin Orzeske, *UFADAA and Privacy*, UNIF. LAW COMM'N, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/UFADAA%20and%20Privacy.pdf (last visited Sept. 5, 2016) (observing that fiduciaries have a duty to "keep private information private, or face liability under our privacy laws.").

247 Rash Letter, *supra* note 43.

the interest of survivors to the information in an account can make privacy a non-factor in the access calculus.

Conversely, drafters of RUFADAA and PEAC considered an account holder's interest in privacy during the process of crafting each model statute. The weight assigned to an account holder's privacy, however, is subject to interpretation. The ULC asserted that "[t]he general goal of the act is to facilitate fiduciary access while respecting the privacy and intent of the account holder,"[248] but then provided personal representatives access to the contents of an online account by default under the terms of UFADAA.[249] Additionally, even though the ULC responded to the privacy criticisms in RUFADAA, the order in which the ULC promulgated its model legislation reflects, in all likelihood, the importance of a deceased account holder's privacy to the drafters. UFADAA granted access by default and *then* RUFADAA offered greater privacy protection for a decedent's digital assets in response to muscular opposition.[250] Under those chronological circumstances, the legislative U-turn does not seem to be driven by a new found commitment to a decedent's right of privacy within the single year separating UFADAA and RUFADAA. Instead, the move from default access to privacy protection appears to be a reaction to a legislative wallop; a display of legislative pragmatism. The ULC cannot be faulted for its pragmatic approach to passing model legislation, but it also cannot claim an unwavering interest in protecting the privacy of decedents' digital information.

Similarly, the arguments of opponents do not evince any great solicitousness for the decedent's privacy interest in account information. PEAC's drafters criticized UFADAA because it "disregard[ed] the privacy interests of third parties and decedents by essentially creating a 'show me everything' rule for whoever becomes a fiduciary."[251] A decedent's interest in privacy, however, is an afterthought compared to the privacy interests of survivors. For example, a Center for Democracy and Technology blog post asserted that UFADAA "raise[d] concerns for third parties who might have communicated with the deceased" because they "may have sent vulnerable or sensitive information to the deceased" without regard to any privacy interest of a decedent.[252] The State Privacy and Security Coalition prioritized the relevant interests in its objection to Connecticut's UFADAA-based bill on the ground

---

248 UFADAA, *supra* note 44, at 2 (Prefatory Note).

249 *Id.*

250 *See supra* notes 226–231 and accompanying text (discussing the changes that the ULC made to UFADAA in response to the strong campaign against it).

251 *Privacy Afterlife*, NETCHOICE, https://netchoice.org/library/decedent-information/ (last visited Aug. 13, 2016).

252 Alethea Lange, *Everybody Dies: What is Your Digital Legacy?*, CTR. FOR DEMOCRACY & TECH. (Jan. 23, 2015), https://cdt.org/blog/everybody-dies-what-is-your-digital-legacy/.

that it had a "complete disregard for the privacy of other persons who communicated with the decedent, as well as the privacy of the decedent."[253] A decedent's privacy interest is not entirely ignored, but it is secondary to the privacy of surviving correspondents.

Casting further doubt on their commitment to post-mortem account privacy, and perhaps privacy as a general matter, UFADAA's service provider opponents intrude upon the privacy of accounts during the lives of their account holders. When Yahoo! implemented a new email system in late 2012, the interface allowed Yahoo! to scan incoming email messages for information that could be used by advertisers to target ads aimed at the account holder.[254] The account holder may not have read the incoming email, but Yahoo!'s software had scoured it for information that might be useful to third parties.[255] And Yahoo! is not alone in such a practice—Google's email software has employed the same scanning technique.[256] In fact, Google's software also (allegedly) sent spam to users that had the appearance of emails, a practice derisively denominated as getting "Scroogled."[257] Humorously, the anti-Google campaign went so far as to have hats, shirts, and mugs emblazoned with "Scroogled," a "Scroogled" website, and a Twitter handle.[258] Moreover, the hunting and gathering of information has expanded as instant messages are also probed for possible violations of copyright law.[259] Regardless of the platform of communication, one privacy analyst observed that "it's the norm that when these companies review their privacy policies that they strip away people's rights rather than protecting them."[260] If user privacy is discounted during that user's life, then service provider assertions that they seek to protect a deceased account holder's privacy are, to say the least, dubious.

---

253 Letter from James J. Halpert, Gen. Counsel, State Privacy and Sec. Coal., Inc., to Senator Eric Coleman and Representative William Tong (Mar. 4, 2015), https://www.cga.ct.gov/2015/JUDdata/Tmy/2015SB-00979-R000306-Halpert,%20James%20J.%20-%20State%20Privacy%20and%20Security%20Coalition,%20Inc.-TMY.PDF.

254 John P. Mello, Jr., *Yahoo Mail Redesign Becomes Permanent, Privacy Issues Surface*, PCWORLD, (June 3, 2013), http://www.pcworld.com/article/2040642/yahoo-mail-redesign-becomes-permanent-privacy-issues-surface.html.

255 *Id.* ("When you choose to use Yahoo's revamped interface, you also agree (unless you opt out) to let the service scan email arriving in your inbox for, among other things, information that can be used to target advertising to you.").

256 *Id.*

257 Mary Jo Foley, *Microsoft Readies a New Scroogled Attack on "Gspam"*, ZDNET (Aug. 9, 2013), http://www.zdnet.com/article/microsoft-readies-a-new-scroogled-attack-on-gspam/.

258 Mary Jo Foley, *Did Microsoft Just Kill its Anti-Google "Scroogled" Campaign?*, ZDNET, (Apr. 14, 2014), http://www.zdnet.com/article/did-microsoft-just-kill-its-anti-google-scroogled-campaign/ (noting that a Gmail user could avoid getting "Scroogled" by adjusting the settings on the account).

259 *See* Mello, *supra* note 254.

260 *Id.*

Whether omitting privacy as a factor in its entirety or expressing support for the protection of posthumous privacy that rings hollow, the debate regarding post-mortem access to a decedent's online accounts largely ignores the interest of the one party who is indispensable to the issue: the decedent.[261] More specifically, arguments mustered to justify privacy positions generally, though not entirely, disregard whether or not an individual intended to have the contents of online accounts remain private after death. From the perspective of the law of wills, the absence of meaningful consideration of a decedent's intent is striking because much of the law of wills is founded on that intent.[262] The Uniform Probate Code, which contains provisions governing both intestate and testate estates, declares that one of its purposes is "to discover and make effective the intent of a decedent in distribution of his property."[263] Whether labeled as "probable intent" for purposes of distributing property for individuals who die without a will or "construed intent" when interpreting a will, the intent of the decedent is nonetheless the foremost goal when distributing an individual's property after death.[264]

While undervaluing an individual's intent in a probate setting runs counter to probate law's focus on decedent intent, the low regard for decedent privacy is in accord with privacy's boundary at common law. Historically, a deceased individual does not have a common law right to privacy because the right of privacy is vindicated by a legal action that is personal to the holder; therefore, the legal right vanishes at the death of the holder.[265] As a result, the estate of a deceased individual is also barred from filing suit for an invasion of a decedent's privacy.[266] Similarly, surviving relatives are also prohibited from seeking redress for an invasion of a decedent's privacy; there

---

261 The word "largely" is used because NetChoice did not entirely ignore a decedent's intent, *see Privacy Afterlife*, *supra* note 251 (arguing that PEAC honors citizens' explicit and implied privacy choices regarding their privacy afterlife).

262 The phrase "much of the law of wills" is used because at least one aspect of the law of wills does not account for the intent of the decedent. Upon marriage, one spouse obtains an elective share of the other spouse's estate at death regardless of how much the decedent spouse wished to disinherit the surviving spouse. In that way, the law of wills ignores the intent of the decedent spouse in favor of a surviving spouse. *See* UNIF. PROBATE CODE § 2-102 (amended 2010).

263 *Id.* § 1-102(b)(2) (UNIF. LAW COMM'N 2013).

264 *See id.* §2 (Prefatory Note).

265 RESTATEMENT (SECOND) TORTS § 652I cmt. b (AM. LAW INST. 1977). *See also* Metter v. L.A. Exam'r, 95 P.2d 491, 494 (Cal. Ct. App. 1939) (describing a lawsuit based upon a violation of privacy as "a purely personal action [that] does not survive, but dies with the person."); Wyatt v. Hall's Portrait Studio, 128 N.Y.S. 247, 249 (N. Y. 1911) ("The peculiarly personal character of the cause of action created by the statute negatives the idea that the Legislature intended that it should be enforceable by the personal representatives of the person in whose favor the cause of action existed. The injury done by the violation of the right does not affect the estate of the person injured, but is strictly an injury to the person of the plaintiff."); Laura Hunter Dietz, 20 MICH. CIV. JUR. PRIVACY § 3 (2015) at 188 (describing the common law right of privacy).

266 RESTATEMENT (SECOND) TORTS § 652I cmt. b (AM. LAW INST. 1977).

is no relational right of privacy.[267] Given the firmly entrenched view that a decedent has no cause of action for an invasion of privacy, minimizing the decedent's privacy interest in crafting the UFADAA, RUFADAA, and PEAC mirrors the traditional understanding of the right of privacy. The legislatively prudent approach is to eschew a decedent's interest and focus on the privacy interests of surviving correspondents because their interests remain protected in both the policies of providers as well as common law, and they can file suit seeking a remedy for a violation.

The historical enforcement barrier to protecting a decedent's *informational* privacy, however, has not proven to be insurmountable. As evidence of the permeability of the death barrier, Congress has enacted federal laws that protect posthumous privacy as an offshoot of the privacy protection afforded to those who survive the decedent, and may suffer harm due to the release of information about the decedent. The Health Information and Privacy Accountability Act of 1996 (HIPPA), for example, includes a Privacy Rule that seeks to balance "important uses of information" with "the privacy of people who seek care and healing."[268] While many of HIPAA's regulations are aimed at the living, HIPAA's disclosure restrictions extend protection to medical information associated with deceased persons.[269] More specifically, a "covered entity" must keep an individual's health information private for fifty years after the individual's death.[270] The fifty-year moratorium balances "the privacy interests of living relatives or other affected individuals with a relationship to the decedent, with the difficulty of obtaining authorizations from personal representatives as time passes."[271] Although the protection is premised on the privacy interests of surviving individuals, a decedent's private medical information is nevertheless generally prohibited from being disclosed.[272] Prohibiting informational disclosure based upon the interests of

---

267 See, e.g., Fitch v. Voit, 624 So. 2d 542, 543 (Ala. 1993) ("[T]he right of privacy is a personal right, and that this Court has not recognized a 'relational right of privacy,' under which the plaintiffs make their claim."); West v. Media Gen. Convergence, Inc., 53 S.W.3d 640, 648 (Tenn. 2001) ("[T]he right to privacy is a personal right. . . . [it] may not be . . . asserted by a member of the individual's family, even if brought after the death of the individual."). For general and historical information about the absence of a relational right of privacy, see Ronald F. Fisk, *Why Not a Relational Right of Privacy?–or Right of Property?*, 42 UMKC L. REV. 175, 175–76, 181–82 (1973).

268 *Summary of the HIPAA Privacy Rule,* U.S. DEP'T. HEALTH & HUM. SERVS., (last visited Aug. 13, 2016), http://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

269 45 C.F.R. § 164.502(g) (2015).

270 *Id.* § 160.103 (excluding information "[r]egarding a person who has been deceased for more than 50 years" from the definition of "[p]rotected health information"); *id.* § 164.512(f) ("A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.").

271 Modification to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5,566, 5,614 (2013) (codified at 45 C.F.R. §§ 160, 164 (2015)). A chief concern that motivated the 50-year period was that archivists and other interested persons had trouble locating a personal representative to authorize discloser of protected health information as time passed. *Id.*

272 *Id.*

survivors yields the same result as basing nondisclosure upon a decedent's interest—nondisclosure.

Despite the general fifty-year ban on disclosure, the Code of Federal Regulations declares that a "covered entity" must treat a personal representative of a decedent's estate like the individual for purposes of HIPAA's privacy protections.[273] Upon first blush, equating the access of a personal representative with that of the individual seems to permit a personal representative to go on a foraging expedition for a decedent's health information. The access granted to personal representatives by HIPAA, however, is not limitless. For example, an individual cannot obtain psychotherapy notes and "[i]nformation compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."[274] More broadly, the Code of Federal Regulations qualifies that a personal representative is treated as the individual "with respect to protected health information relevant to such personal representation."[275] And, HIPPA "does not override or interfere with State or other laws that provide greater protection" for "sensitive" medical infor-

---

273 45 C.F.R. § 164.502(g)(1) (2015).

274 *Id.* § 164.524(a)(1)(i) (2015). *See also, e.g., HIPPA Privacy Policy*, FLOYD MEMORIAL HOSP., (June 26, 2014) http://floydmemorial.com/hipaa/ ("You have the right to inspect and obtain a copy of the PHI that may be used to make decisions about you, including patient medical records and billing records, but not including psychotherapy notes. . . . You have the right to request an 'accounting of disclosures.' An 'accounting of disclosures' is a list of certain non-routine disclosures we have made of your PHI. This list will not include uses you have already authorized, or those for treatment payment or operations. This list will not include psychotherapy notes, or uses made for national security purposes, or, to corrections or law enforcement personnel."); *HIPPA, Minnesota's Health Records Act, and Psychotherapy Notes*, MINN. DEP'T. HEALTH (Oct. 2014), http://www.health.state.mn.us/e-health/privacy/ps102114psychotherapy.pdf ("Under HIPAA's Privacy Rule, a mental health professional is not required to disclose psychotherapy notes to a patient. In fact, psychotherapy notes are specifically excluded from a patient's general right to access or inspect their own medical records If a mental health professional ever wishes to disclose the psychotherapy notes, however, they are permitted to do so, but must first receive the patient's authorization."); *Confidentiality of Psychotherapy and Personal Notes*, COLUM. U. MED. CTR. (Dec. 2009), http://www.cumc.columbia.edu/hipaa/pdf/Psychotherapy_Notes_Policy.pdf ("Psychotherapy and personal notes are considered the property of the health care provider who created them, and will not be released or disclosed to patients.").

275 45 C.F.R. § 164.502(g)(4) (2015) ("If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation."). *See also, e.g., HIPAA For Professionals, FAQ, 1503—Does HIPAA Permit a Covered Entity to Disclose PHI About a Decedent to Family Members*, U.S. DEPT. HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/faq/1503/does-hipaa-permit-a-covered-entity-to-disclose-information-about-a-decedent/index.html (last accessed Aug. 14, 2016). For more information about HIPAA and the privacy of decedents, see Jacqueline Myles Crain, *HIPAA—A Shield For Health Information and a Snag for Estate Planning and Corporate Documents*, 40 REAL PROP. PROB. & TR. J. 357, 366 (2005); Leslie P. Francis, *Skeletons in the Family Medical Closet: Access of Personal Representatives to Interoperable Medical Records*, 4 ST. LOUIS U. J. HEALTH L. & POL'Y 371, 378-80 (2011).

mation related to "HIV/AIDS, substance abuse, or mental health information."[276] As a result, "[c]overed entities may continue to provide privacy protections to decedent information."[277] During the course of estate administration, the personal representative might need access to health records to identify debts accruing from medical services, but not information unnecessary to settle the estate.

Like HIPPA's asymptotic recognition of posthumous privacy, the Freedom of Information Act of 1996 (FOIA) also permits a decedent's information to remain private by indirect means.[278] In response to a breakdown of the information flowing to the public under the Administrative Procedure Act,[279] FOIA's section 552(a)(3)(A) mandates that agencies furnish copies of records to citizens who make requests that "reasonably describe" the desired record as well as comply with any published rules that govern the submission of requests.[280] Furthermore, federal agencies are directed to employ a "presumption of openness when responding to a FOIA request."[281] Notably, a requesting person need not identify a reason for the request,[282] which presumably makes it easier to submit a request. To that end, the number of requests made to specific federal agencies is directly proportional to the political controversy associated with the regulatory ambit of the federal agency. The United States Citizenship and Immigration Services received 143,794 requests during the 2014 fiscal year while the Office of Operations Coordination fielded a mere 59 requests during the same period.[283] Despite the volume of requests and the time consumed to respond, each branch of the federal government lauds FOIA "as a vital part of our democracy."[284] As evidence of the importance of citizens' access to information, every state has enacted a version of FOIA to provide citizens with access to state records.[285]

While FOIA creates a blanket mandate favoring disclosure, two exemptions serve as buffers against disclosure thereby protecting personal privacy. Exemption six shields data in "personnel and medical files and similar files" from disclosure when revealing the information "would constitute a clearly

---

276 78 Fed. Reg. 5,566, 5,614 (2013).

277 *Id.*

278 *See* 5 U.S.C. § 552 (2012).

279 *See* H.R. REP. NO. 1497-89, pt. 3, at 25, 27 (1966) (concluding that the APA had become "authority for withholding, rather than disclosing information" and "improper denials" occurred repeatedly).

280 5 U.S.C. § 552(a)(3)(A) (2012).

281 U.S. Dep't. of Justice, FOIA.GOV, http://www.foia.gov/about.html (last visited Aug. 10, 2016).

282 *See, e.g.*, U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 771 (1989).

283 U.S. Dep't. of Justice, FOIA.GOV, http://www.foia.gov/data.html#foiaReportsTable (last visited Aug. 10, 2016).

284 U.S. Dep't. of Justice, FOIA.GOV, http://www.foia.gov/about.html (last visited Aug. 10, 2016).

285 Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution,* 86 MINN. L. REV. 1137, 1161 (2002) ("Today, all fifty states have open records statutes, a majority of which are modeled after the FOIA.").

unwarranted invasion of personal privacy."[286] In a similar vein, exemption seven prohibits the acquisition of personal information to be used for "law enforcement purposes" when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[287] Applying either exemption requires a court to balance the individual's interest in personal privacy with the public's interest in disclosure.[288] Furthermore, a "presumption" in favor of disclosure is deployed when applying exemption six and the language of exemption seven limits its application to purposes involving "law enforcement."[289] In short, the scales used by courts to weigh privacy versus disclosure tilt heavily in favor of disclosure under the FOIA.

Given FOIA's *inter vivos* protection of personal privacy under its exemptions, a question arises regarding whether or not the protection of individual privacy survives death under the exemptions. The Department of Justice clarified the applicability of the exemptions to the privacy of decedents in a 1982 update.[290] Because privacy rights end at death, according to the update, the exemptions do not "directly" apply to protect a decedent's privacy.[291] However, "careful consideration should be given to whether such protection can be extended to others."[292] To that end, the Department of Justice observed that

> [W]hile privacy rights cannot be inherited by one's heirs, the disclosure of particularly sensitive personal information pertaining to a deceased person may well threaten the privacy interests of surviving family members or other close associates.[293]

Although it may be derived from the privacy rights of survivors, a decedent's privacy regarding some information is retained after death; indirect protection is again nonetheless protection. Simply put, "Congress intended

---

286 5 U.S.C. § 552 (b)(6) (2012).

287 5 U.S.C. § 552 (b)(7)(C) (2012).

288 U.S. Dep't. of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 762 (1989) ("Exemption 7(C) requires us to balance the privacy interest in maintaining, as the Government puts it, the 'practical obscurity' of the rap sheets against the public interest in their release."); Multi Ag Media LLC v. Dep't. of Agric., 515 F.3d 1224, 1229 (D.C. Cir. 2008) ("The balancing analysis for FOIA Exemption 6 requires that we first determine whether disclosure of the files 'would compromise a substantial, as opposed to *de minimis,* privacy interest,' because 'if no significant privacy interest is implicated FOIA . . . demands disclosure.'") (quoting Nat'l Ass'n of Retired Fed. Emps. v. Horner, 879 F.2d 873, 874 (D.C. Cir. 1989)).

289 Law. Comm. for Civil Rights of S.F. Bay Area v. U.S. Dep't. of the Treasury, No. C 07-2590 PJH, 2008 WL 4482855, at *19–21 (N.D. Cal. 2008).

290 *FOIA Counselor: Questions and Answers*, U.S. DEP'T. OF JUSTICE (Jan. 1, 1982), http://www.justice.gov/oip/blog/foia-update-foia-counselor-questions-answers-24.

291 *Id.*

292 *Id.*

293 *Id.*

that the privacy interest protected under FOIA extend beyond the common law."[294]

The Department of Justice's admonition to weigh the impact of disclosure on a decedent's survivors is not without effect on judicial decision-making. To the contrary, courts frequently consider the consequences of public knowledge of the protected information and opt to protect the privacy rights of survivors, which, in turn, protects the privacy of decedents. A federal court, for example, determined that Exemption 7(C) shielded Dr. Martin Luther King Jr.'s survivors from the ramifications of disclosing "information of a personal nature, the disclosure of which allegedly could embarrass Dr. King's family and associates or damage their reputations."[295] Similarly, a federal court found that Exemption 6 prohibited the release of x-rays and photographs associated with President Kennedy's autopsy to prevent the "anguish" that may be inflicted upon the surviving Kennedys following disclosure.[296] Of course, an individual need not be a public figure to benefit from FOIA's exemptions and not all cases result in withholding information from the public.[297] Regardless of the deceased individual's notoriety, a court balances the "public's broad right to information guaranteed under FOIA against the privacy rights which Congress intended to protect" when applying FOIA's exemptions.[298]

As a theoretical matter, HIPPA and FOIA's strategy of protecting a decedent's information as a tangent to protecting a survivor's privacy interest could protect a decedent's interest in the privacy of the contents of digital accounts after death. Arguably, accounting for a decedent's interest in privacy during the legislative process is unnecessary because a deceased account holder's privacy interest is sufficiently vindicated by the legal remedy afforded surviving correspondents. Section 2707(a) of the SCA states that any "person aggrieved by any violation of this chapter . . . may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate."[299] As a result, surviving senders of communications that remain in an online account after the death of an account holder could file suit to enforce their interests in the privacy of their communications. Like the protective schemes of HIPPA and

---

294 Marzen v. Dep't. of Health & Hum. Servs., 825 F.2d 1148, 1152 (7th Cir. 1987).

295 Lesar v. U.S. Dep't. of Justice, 636 F.2d 472, 486 (D.C. Cir. 1980) (construing Exemption 7(c)).

296 Katz v. Nat'l Archives & Records Admin., 862 F. Supp. 476, 483–86 (D.D.C. 1994).

297 *See Marzen*, 825 F.2d at 1153–54 (barring the release of an infant's medical records under 7(c)); Outlaw v. U.S. Dep't. of Army, 815 F. Supp. 505, 506 (D.D.C. 1993) (ruling that the potential harm from release was outweighed by the public interest in disclosure as a check on the administration of justice). For a collection of cases where a court weighs the public interest in disclosure against the privacy interest of survivors, see U.S. DEP'T. OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT: EXEMPTION 6 14 n.54 (last updated Jan. 10, 2014), https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption6.pdf.

298 *Marzen*, 825 F.2d at 1154.

299 18 U.S.C. § 2707(a) (2012).

FOIA, shielding a decedent's account from any disclosure could be a byproduct of the primary protection afforded surviving individuals who have information stored in the decedent's account.

Relying on survivors to protect the privacy of their messages in a decedent's online account, however, falls short of providing full protection for the information remaining in a decedent's online account. An individual correspondent could file suit seeking to enforce the protection offered by the SCA, but the correspondent could only protect information in which the correspondent has an interest. Obviously, digital accounts that serve as platforms of communication typically store information sent from a large number of parties. Because a decedent's intent regarding privacy may be unknown, protecting the entirety of the information that a decedent intended to keep private would require the collective action of all correspondents to seek and receive "relief as may be appropriate."[300] Some correspondents, of course, will not file suit for any number of reasons, even though the decedent may have wanted the information to remain private. In reality, protecting a decedent's account information as a corollary to the protection granted to information in the decedent's account connected to living persons is impractical.

One reason that a surviving correspondent may fail to protect her interest in the information stored in a decedent's account is straightforward—individuals who communicated with the account holder may have no idea that the account holder is, in fact, dead. Indeed, information associated with a deceased user may appear in a living person's interface, which gives the false impression that the deceased user is alive.[301] As a consequence, a living correspondent may send innocuous birthday greetings or innermost thoughts without knowing that the recipient of the information has died.[302] If a correspondent does not know that an account holder is deceased, then the correspondent has no reason to seek protection for information in the decedent's account, particularly within any given limitations period. The informational asymmetry regarding the status of the account holder undermines the ride-along protective strategy to post-mortem access/disclosure of digital assets.

In addition to collective action and informational problems, the information disclosed to a personal representative or survivors could be interpreted differently than was intended by a decedent. Disclosure of the contents of digital accounts risks misinterpretation because digital information "can be emotionally impoverished when it comes to nonverbal messages that add

---

300 *Id.* § 2707(b)(1) (2012)

301 Jaweed Kaleem, *Death on Facebook Now Common As 'Dead Profiles' Create Vast Virtual Cemetery*, HUFFINGTON POST (Jan. 16, 2013), http://www.huffingtonpost.com/2012/12/07/death-facebook-dead-profiles_n_2245397.html (recounting that birthday wishes that were posted for a deceased individual); Buck, *supra* note 107 (observing that "[m]any profiles continue to surface in Sponsored Stories, which promotes users' activity and likes from months and years past" even though user may be deceased).

302 Kaleem, *supra* note 301.

nuance and valence to our words."[303] In other words, digital information does not permit the receiver of the digital data to use her "social radar" to decipher the sender's intent.[304] In fact, a study of the use of email among co-workers found that "[e]mail characteristics make miscommunication likely," recipients of emails "misinterpret work emails as more emotionally negative or neutral than intended," and the use of email as a primary means of communication increases the likelihood of conflict.[305] The closeness of the relationship between the correspondents may reduce the risk of misinterpretation,[306] but the risk is ever-present. Disclosing the contents of a decedent's digital accounts provides the raw data, but cannot convey the situational context in which that data was created; therefore, the true intent of a deceased correspondent may be irretrievably lost.

A recent example illustrates the contextual nature of digital communications and the potential risks of post-mortem disclosure of the content of digital accounts. Sony Pictures Entertainment experienced a "brazen cyber-attack," that resulted in the public release of the content of numerous emails stored on Sony's system.[307] While some of the emails contained information protected by HIPAA,[308] other messages contained information that the sender/recipient would likely want to remain private even though the content was not protected by federal or state law.[309] Messages that labeled popular Hollywood figures in less than glowing terms or contained racially insensitive remarks were intended for the recipient's eyes alone.[310] The release of the content of the messages to the public prompted one of the sender/recipients to comment that the emails were "not an accurate reflection" of the

---

303 Daniel Goleman, *Email is Easy to Write (And to Misread)*, N.Y. TIMES (Oct. 7, 2007), http://www.nytimes.com/2007/10/07/jobs/07pre.html?_r=1&ex=1349496000&en=f988d525510cfle0&ei=5090&partner=rssuserland&emc=rss&oref=slogin.

304 *Id.*

305 Kristin Byron, *Carrying Too Heavy a Load? The Communication and Miscommunication of Emotion by Email*, 33 ACAD. OF MGMT. REV. 309, 309 (2008).

306 *See* Goleman, *supra* note 303.

307 Letter from Sony Pictures to Current and Former Sony Pictures Employees and Dependents, and Production Employees (Dec. 15, 2014), http://www.sonypictures.com/corp/notification/SPE_Cyber_Notification.pdf.

308 *Id.*

309 *See* Amanda Hess, *Inside the Sony Hack*, SLATE (Nov. 22, 2015), http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html; Eugene Volokh, *Can Sony Sue Media Outlets who Publish the Stolen Sony Documents?*, WASH. POST (Dec. 15, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/15/can-sony-sue-media-outlets-who-publish-the-stolen-sony-documents/?utm_term=.f3404f89f27b.

310 *See* Alex Steadman, *Leaked Sony Emails Reveal Nasty Exchanges and Insults*, VARIETY (Dec. 9, 2014), http://variety.com/2014/film/news/leaked-sony-emails-reveal-nasty-exchanges-and-insults-1201375511/ (detailing various insults directed at Hollywood figures).

sender and "written in haste without much thought or sensitivity."[311] Despite the effort at damage control, the unintended publication of the content triggered an "unraveling of relationships in Hollywood" and "disrupted the web of executive, business and talent relationships that stitches together Sony's core moviemaking operation."[312]

Whatever the Sony correspondents meant by the language in their emails, they had an opportunity to explain any misunderstanding that accompanied disclosure. A decedent, by contrast, has no chance to attempt to control the damage by explaining what was intended by the information or the context in which it was created. And although the damage threatened by disclosing content during estate administration may not have the potential for financial repercussions like gossipy Hollywood emails, disclosed information could be just as personally damaging for survivors. Learning about a decedent's view of a relationship with a survivor that differs from the survivor's expectation and recollection, or offhand comments made in jest but misinterpreted, threaten the types of emotional and mental harm comprehended by both HIPPA and FOIA.[313] The damage is immune from explanation by a decedent once the subject of a private communication learns the content of the communication.

Each of the foregoing problems—collective action, misinterpretation, and possible harm from disclosure—unavoidably affects the issue of postmortem access and disclosure of a record or contents of digital assets due to the nature of digital communication. Digital assets used for the purpose of

311 Christopher Rosen, *Scott Rudin and Amy Pascal After Racially Insensitive Emails About Obama Leak*, HUFFINGTON POST (Dec. 11, 2014), http://www.huffingtonpost.com/2014/12/11/scott-rudin-amy-pascal-apology_n_6310040.html.

312 Michael Ceiply & Brooks Barnes, *Sony Hacking Fallout Includes Unraveling of Relationships in Hollywood*, N.Y. TIMES (Dec. 18, 2014), http://www.nytimes.com/2014/12/19/business/media/sony-attack-is-unraveling-relationships-in-hollywood.html?_r=0 (detailing the impact of the hacking and release on the personal and professional relationships).

313 The tragic case of Tyler Clementi, a college student who committed suicide after his roommate "electronically spied" on an intimate encounter with a webcam, provides an example of the possible harm associated with posthumous discovery of information, albeit in a non-probate context. Prior to his death, Tyler wrote that his mother had "rejected him" after learning he was gay. Although the information about Tyler's mother emerged in conjunction with a criminal investigation, it is not difficult to imagine that the information caused some degree of emotional harm to Tyler's mother. In fact, Tyler's mother has reviewed her interactions with her son in an effort to understand his digital comments. And for his part, though one can never know for certain, Tyler is not likely to have wanted his mother to learn his intimate thoughts on her reaction to their discussion – at least by way of an online post. Indeed, Tyler offered his view of his mother's feelings in a digital platform presumably outside the ready access of his mother. In other words, Tyler commented in private, but now those comments have become known by the subject of the comments. *See* Ian Parker, *The Story of a Suicide*, NEW YORKER MAG. (Feb. 6, 2012), http://www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide (indicating that the information regarding the mother's reaction may have been included in a "post"); Kashmir Hill, *The Post-Mortem Privacy Invasion of Tyler Clementi*, YAHOO NEWS (Aug. 15, 2011), https://www.yahoo.com/news/post-mortem-privacy-invasion-tyler-clementi-160116484.html?ref=gs (stating that "private chats revealing his mother's rejection of his sexuality and racist statements about his roommate are now being exposed" and describing the feelings of Tyler's mother after learning Tyler was gay).

communication are co-constructed. Facebook accounts, instant messaging interfaces, and email accounts contain information in the form of sent messages from account holders as well as messages received from correspondents that remain in the account by default. As a result, an individual's account not only stores information generated by the account holder, but also content generated by another individual. If the privacy of those communications is not preserved at death, some people may suffer unintended harm. Moreover, information that a decedent freely offered to one party may not have been intended for any other party; privacy is contextual. The critical contextual factor for purposes of property distribution at death is decedent intent regarding digital assets. Given the enforcement problems, the only way to protect a decedent's intent regarding the privacy of digital accounts and prevent unintended harm may be to build a firewall that surrounds an individual's accounts after death. At the very least, an individual's independent interest in posthumous privacy should factor into the construction of the legal framework for access to post-mortem access to digital assets.

III. POSTHUMOUS PRIVACY AND RECALIBRATING DIGITAL ASSET LEGISLATION

Isolating a decedent's independent and surviving interest in privacy does not automatically activate post-mortem protection from disclosure during estate administration. Instead, the privacy setting must be calibrated in accordance with the primary functions that undergird both intestate and testate succession. Whether property is to be distributed by intestate statute or by will, the basic interpretive function of the law of wills is to effectuate a decedent's intent regarding the distribution of her property.[314] Other goals may exist, such as promoting family harmony via intestate distribution,[315] but giving effect to a decedent's intent is generally accepted as the core principle of the law of wills.

---

314 UNIF. PROBATE CODE §1-102(b)(2) (amended 2010).

315 *See, e.g.*, Mary L. Fellows et al., *Committed Partners and Inheritance: An Empirical Study*, 16 LAW & INEQ. 1, 8 (1998) ("At the same time that intestacy statutes reflect social norms and values, they also shape the norms and values by recognizing and legitimating relationships."); E. Gary Spitko, *The Expressive Function of Succession Law and the Merits of Non-Marital Inclusion*, 41 ARIZ. L. REV. 1063, 1102 (1999).

A. *Intestacy and Default Intent*

According to statistics, most people die intestate;[316] therefore, a state's statute of descent and distribution governs the allocation of a vast amount of probate property. As a general matter, intestacy statutes identify the individuals entitled to share in a decedent's estate, the order in which they take their shares, and the amount each individual shares.[317] Although described as a "theoretical grab bag" by scholars,[318] courts generally agree that a fundamental goal of intestate statutes is to distribute a decedent's property in a manner that comports with how a decedent would have distributed her property if the decedent had executed a valid will.[319] Because an intestate's actual intent cannot be known, intestate statutes allocate property without regard to a decedent's specific intent.[320] As a result, the possibility of a mismatch between an individual's specific and likely intent has served as the basis for robust criticism of intestate statutes.[321] Nevertheless, courts routinely opine that the purpose of statutes of descent and distribution is to allocate property pursuant to a decedent's probable intent.

The challenge of discerning an account holder's probable intent regarding post-mortem access is heightened by the terms of service agreements that

---

316 *See* Richard Eisenberg, *Americans' Ostrich Approach to Estate Planning*, FORBES (Apr. 9, 2014), http://www.forbes.com/sites/nextavenue/2014/04/09/americans-ostrich-approach-to-estate-planning/#4ca8cc1df07b.

317 *See, e.g.*, UNIF. PROBATE CODE § 2-101 (amended 2010).

318 Adam J. Hirsch, *Default Rules in Inheritance Law: A Problem in Search of Its Context*, 73 FORDHAM L. REV. 1031, 1036 (2004); *See also* Mary L. Fellows et al., *Public Attitudes About Property Distribution at Death and Intestate Succession Laws in the United States*, 1978 AM. BAR FOUND. RES. J. 321–22, 323–24.

319 *See, e.g.*, *In re* Estate of Griswold, 24 P.3d 1191, 1195 (Cal. 2001) ("[T]he proposed comprehensive legislative package to govern wills, intestate succession, and related matters would 'provide rules that are more likely to carry out the intent of the testator or, if a person dies without a will, the intent a decedent without a will is most likely to have had'"). This is not meant to suggest that a decedent's intent is unanimously embraced as the primary goal of intestate succession, *see*, Mary L. Fellows, *Concealing Legislative Reform in the Common-Law Tradition: The Advancements Doctrine and the Uniform Probate Code*, 37 VAND. L. REV. 671, 674 n.8 (1984); E. Gary Spitko, *An Accrual/Multi-Factor Approach to Intestate Inheritance Rights for Unmarried Committed Partners*, 81 OR. L. REV. 255, 289 (2002).

320 *In re* Lyon's Will, 2 N.E.2d 628, 630 (N.Y. 1936) ("The Legislature may by statute create a general rule for the distribution of the property of a decedent in case of intestacy. The general rule so formulated cannot take into account the desires or intentions of a particular decedent. Such desires or intentions are ineffective unless expressed in a will properly executed and which conforms to the limitations placed by law upon the testamentary power of the decedent. The courts give effect to a testamentary intent so expressed; where there is no such expression of intent the decedent's property must be distributed according to the general rule created by the Legislature.").

321 *See, e.g.*, Alyssa A. DiRusso, *Testacy and Intestacy: The Dynamics of Wills and Demographic Status*, 23 QUINNIPIAC PROB. L. J. 36 (2009) (compiling data to compare to intestate distributions by statute and identifying criticisms of intestate statutes).

permit individuals to become account holders. Some terms of service agreements spell out what happens to the contents of an account once the holder dies. Yahoo!'s terms of service, at issue in the Ellsworth dispute, declare that an account is "non-transferable and any rights to your . . . content within your account terminates upon your death."[322] While many, probably most, soon-to-be account holders do not read the terms of service, any given decedent may have, in fact, relied on the agreement to communicate intimate thoughts in some messages that she would not have wanted to become known after death. On the other hand, a decedent may have preferred to transfer all of the account's contents to her survivors at death so that they could learn about her life. Regardless, some terms of service agreements are silent about the treatment of the account following the account holder's death. Under such circumstances, a decedent may have mistakenly assumed either that the privacy of the password-protected account would survive death or that all of the account's contents would be transferred at death. With or without a provision in the terms of service that governs post-mortem consequences following an account holder's death, divining a decedent's intent boils down to making a decision between two plausible choices with incomplete information as a guide.

Recognizing the utility of empirical data as a tool to develop the Uniform Probate Code,[323] NetChoice commissioned a study to discover what people thought about post-mortem privacy of digital accounts.[324] Zogby Analytics conducted an online survey of 1,012 adults during January 2015 that consisted of six questions about the respondents' views of privacy of online information after death.[325] According to NetChoice's interpretation of the survey's results,

> More than 70 percent of Americans think that their private online communications and photos should remain private after they die—unless they gave prior consent for others to access. In addition, 70 percent also felt that the law should err on the side of privacy when someone dies without documenting their preference about how to handle their private communications and photos.[326]

Given the results of the survey, NetChoice concluded, "Americans say that their right to privacy does not end when they take their last breath, and believe that maintaining the privacy of their electronic communications trumps giving access to family and heirs."[327]

---

322 *See Yahoo Terms of Service*, *supra* note 105.

323 Martin L. Fried, *The Uniform Probate Code: Intestate Succession and Related Matters*, 55 ALB. L. REV. 927, 929–31 (1992) (describing the ULC's use of empirical data during the drafting of the Uniform Probate Code).

324 *Privacy Afterlife*, *supra* note 251 (stating that the poll was "conducted by Zogby Analytics for NetChoice").

325 *Id.*

326 *Id.*

327 *Id.*

Although the numerical results seemingly support NetChoice's position on post-mortem privacy, the survey's results may not be as unambiguous as NetChoice's conclusion indicates. Ignoring any argument that NetChoice paid for results that happened to match its legislative position,[328] the questions and possible answers associated with the survey's two primary conclusions suggest more modest conclusions than NetChoice drew from the data. The first question relied upon for NetChoice's two chief conclusions asked "[a]fter a person dies which of the following describes your view when it comes to keeping the emails and instant messages along with digital photos they have sent private?"[329] The available responses to the question included (with percentage of respondents in agreement):

1. My online communications and photos should remain private. I wouldn't want anyone accessing them after I die, unless I gave prior consent. (70.5% agreed)
2. Estate attorneys and executors should control my private communications and photos even if I didn't give prior consent. (15.2% agreed)
3. Not sure (14.4 % agreed)[330]

Thus, NetChoice decided that 70% of respondents favored post-mortem privacy in the absence of express permission to access the contents of digital accounts after an account holder's death.

The problem with the general conclusion that 70% of respondents prefer privacy over access in general terms is that it exceeds the framework of the question. The question asked about post-mortem privacy associated with information "they have sent," but did not capture a respondent's view of post-mortem privacy of incoming messages.[331] A possibility exists that an individual may have differing views of privacy associated with outgoing and incoming mail. On one hand, the expansive storage capability and password protection of email and instant message accounts may have expanded the expectation of privacy to include both outgoing and incoming information. If so, the omission of respondents' views of post-mortem privacy of incoming messages could be inconsequential. On the other hand, a sender may place a greater value on the privacy of outgoing messages because they contain the sender's thoughts whereas incoming messages contain a correspondent's thoughts.[332] As a result, an individual may desire post-mortem privacy for

328 *Compare id.* (stating that the poll was "conducted by Zogby Analytics for NetChoice"), *with* PEAC, *supra* note 54.

329 *Privacy Afterlife*, *supra* note 251.

330 *Id.*

331 *Id.*

332 This is not intended to suggest that nothing can be gleaned from incoming messages. To the contrary, access to incoming information may provide a great deal of information about the message that

outgoing information while simultaneously having less concern about post-mortem access to incoming information. In fact, the dichotomy exists in the real world, as outgoing and delivered mail is private because it cannot be retrieved, but incoming and received mail can be privately retained during life with the intent that it be discovered at death.[333] The probability that respondents differentiate privacy by distinguishing between outgoing and incoming messages might be low, but it also might not be zero. In any event, adding the words 'or received' to the survey question would account for the possibility and more accurately gauge what respondents thought about post-mortem privacy.

Similarly, the other question associated with NetChoice's primary conclusions does not precisely match the conclusion drawn by NetChoice. The survey question stated "[s]ince 1986, a federal law has prioritized privacy of electronic communications such as email. But now trusts and estates attorneys want new laws giving them control over private communications when a person dies. In your opinion, what should be the priority?"[334] The three available responses to the question included (with percentage of respondents in agreement):

1. Privacy should be the priority. We may not know whether a deceased person wanted family or friends to see their private communications and photos. (70.2% agreed)
2. Access should be the priority. It doesn't matter whether or not the deceased person wanted family or friends to see their private communications and photos – all of it should be available for family and heirs to see. (14.4% agreed)
3. Not sure. (15.5% agreed).[335]

From this data, NetChoice maintained that 70% of those surveyed believed that the law should protect privacy after death in the absence of any indication from the decedent about how death affected the management of the contents of online accounts.

Although the results again seemingly support NetChoice's conclusion that posthumous privacy is preferred, the language used in both the question and the responses leave doubt about the firmness of the conclusion. The question declares that "trusts and estates attorneys" want "new laws giving them control" over a decedent's digital accounts.[336] Using the phrase "giving them

---

was sent to the correspondent. Nevertheless, certainty about the information sent is beyond reach in the absence of the outgoing message.

333 Bruce Feiler, *Secret Histories*, N.Y. TIMES (Jan. 17, 2014), http://nyti.ms/1jaNYMW (containing several stories about secrets that were preserved during life but intended to be revealed at death. According to the story, "some things are too painful to discuss while people are living but too important to be left unsaid after they die").

334 *Privacy Afterlife*, *supra* note 251.

335 *Id.*

336 *Id.*

(attorneys) control" makes it sound as if attorneys will use the information stored in the account for whatever purpose is desired. Attorneys, of course, do not control a decedent's property for their own purposes and few persons would likely want an attorney, who may be a stranger, to have "control over private communications when a person dies."[337] As a result, the possibility exists that respondents chose their answers based upon fear that an attorney or stranger would control information after death rather than an undiluted general desire to prohibit all access to digital contents after death. Given the phrasing of the questions and answers, privacy may be preferred in a qualitative sense, but the quantitative strength of that preference is questionable. And the quantitative differential matters—the conclusion would not be nearly as strong if privacy was preferred by a plurality of the study's respondents.

Whatever the value of Zogby's research study, and some data is better than no data, the mechanics of probate provide a basic reason to establish a default rule of nondisclosure for persons who die intestate without surveys or statistics. In many cases, an intestate individual's personal representative will be a person close to the decedent, such as a spouse, parent, or an adult child. Indeed, such individuals are identified as eligible personal representatives by statute if an individual dies intestate.[338] A strong possibility exists, then, that private communications stored in a decedent's online account contain private information about the very person who will be given access to the account following the death of the account holder. Some messages will be off-hand, even snarky, remarks about a personal representative that may not be particularly informative or hurtful. But other messages may contain more intimate information about the personal representative that a decedent never intended to reveal to individuals other than the recipient of the message.[339] Under those circumstances, the fiduciary duties governing the actions of a personal representative's fiduciary duties do not provide a remedy because disclosure occurred while the personal representative fulfilled her duties. In such cases, which would likely be a majority of probate proceedings given the number of intestate estates, access equals distribution and a risk of subsequent harm.

Ultimately, a personal representative need not "broadcast the information to the world" to breach a decedent's interest in privacy.[340] Information that the decedent did not want known by anyone other than a correspondent

---

337 *Id.*

338 *See, e.g.*, KY. REV. STAT. ANN. § 395.040 (2016) (identifying a spouse and then others entitled to a share of the estate as eligible for appointment as a personal representative); NEV. REV. STAT. § 139.040 (2015) (listing the order of priority as surviving spouse, children, father or mother, brother or sister, grandchildren, anyone else entitled to take by intestacy); WASH. REV. CODE § 11.28.120 (2016) (specifying the order of priority as surviving spouses, children, father or mother, brothers or sisters, grandchildren, nephews and niece, and then others who are not related to the decedent by blood).

339 *See, e.g.*, *supra* notes 307–313 and accompanying text (discussing the emotional and mental harm that can result from disclosing intimate communications).

340 *See* Blachly, *supra* note 246, at 19.

might be disclosed unless a decedent's intent for posthumous privacy is recognized and protected in addition to the protections afforded surviving correspondents. One's imagination need not stretch all that far to think that private thoughts about a personal representative, who is likely to be a family member, in an online account may be hurtful if discovered by the personal representative. Furthermore, providing access by default risks wider distribution because of the possibility that the party learning the contents intentionally or unintentionally disseminates the information. As a result, the only way to avoid the potential for harm to an intestate decedent's interest in posthumous privacy is to set the default on the nondisclosure end of the privacy spectrum.

B. *Testamentary Intent, RUFADAA, and PEAC*

Unlike intestate law's distribution according to a decedent's probable intent, the probate of a valid will allocates property pursuant to a decedent's intent as expressed by the four corners of the instrument. The law from every corner of the nation describes a testator's intent as the bedrock of interpreting wills. For example, Maine's code succinctly provides that "[t]he intention of a testator as expressed in his will controls the legal effect of his dispositions."[341] Similarly, published opinions proclaim hallowed reverence for testator intent in the interpretation of wills by extolling the search for a testator's intent as the "cardinal rule" or the "cardinal principle" of will interpretation.[342] The Supreme Court of North Carolina announced that "[t]he intent of the testator is the polar star that must guide the courts in the interpretation of a will."[343] Presumably conveying the same idea, the Supreme Court of Pennsylvania referred to the intent of a testator as a "polestar" that must "prevail" when interpreting a will.[344] Whether a "cardinal rule," a "cardinal principle," or some permutation of a phrase describing a luminous body in the sky, the

---

341 Me. Stat. tit. 18, §2-603 (2015). *See also* WASH. REV. CODE ANN. §11.12.230 (West 2015) (commanding "due regard" for testator's "true intent"); MO. ANN. STAT. §474.430 (West 2016) (identical to Washington's provision); N.D. CENT. CODE ANN. § 30.1-09-03 (West 2015) ("The intention of a testator as expressed in the testator's will controls the legal effect of the testator's dispositions"); NEB. REV. STAT. § 30-2341 (West 2016) (identical to North Dakota's provision); OR. REV. STAT. § 112.227 (West 2016) (identical to North Dakota's provision).

342 *In re* Estate of Bair, 341 N.W.2d 188, 189 (Mich. Ct. App. 1983) (using the phrase "cardinal rule"); *In re* Williams' Estate, 242 N.W.2d 612, 615 (Neb. 1976) (discussing the "cardinal principle" of will interpretation).

343 Adcock v. Perry, 290 S.E.2d 608, 611 (N.C. 1982) (quoting *Wing v. Wachovia Bank & Trust Co.*, 272 S.E.2d 90 (N.C. 1980)).

344 *In re* Schappell's Estate, 227 A.2d 651, 652 (Pa. 1967) (quoting *In re* Houston Estate, 201 A.2d 592, 595 (Pa. 1964)).

bottom line is that the intent of a testator controls the distribution of the testator's estate.[345]

NetChoice now lauds RUFADAA because it "[h]onors citizens' explicit . . . choices regarding their privacy afterlife,"[346] but 'if requested' court orders erode RUFADAA's commitment to testator intent. Even if a decedent left a validly executed will that unambiguously directs disclosure of account contents, an online service provider possesses the authority to require a court order before complying with the testator's intent under RUFADAA. Seeking a court order to establish that "the user consented to disclosure of the content" or that "disclosure of the content . . . is reasonably necessary for administration of the estate" is redundant when a decedent has a validly executed will with a valid disclosure provision.[347] The disclosure provision in a decedent's will represents a decedent's consent. Furthermore, disclosure is not "reasonably necessary" for estate administration when a will contains a valid disclosure provision, but is instead simply "necessary" to administer a testator's estate pursuant to a testator's intent.[348] The same is true under PEAC, in that a court order to establish that a "request is not in conflict with the deceased user's will" or that the decedent "expressly consented to the disclosure" is unnecessary if a decedent's validly executed will directs disclosure.[349] Given that many state statutes command personal representatives to settle decedents' estates "expeditiously," if requested and mandatory court orders are unnecessary roadblocks to honoring a testator's intent regarding disclosure in the absence of a reason to doubt that intent.[350]

Although court orders are only required if requested under RUFADAA, the fiscally responsible and legally prudent strategy for online service providers fielding requests for either a record or contents under RUFADAA is

---

345 For other expressions of adherence to testator's intent, see First Nat. Bank of Ga. v. Jenkins, 345 S.E.2d 829, 830 (Ga. 1986) ("The court will look to the intent of the testator when construing the language of a will and, whenever possible, the intent of the testator will govern the outcome"); Conover v. Cade, 112 N.E. 7, 10 (Ind. 1916) ([I]n the construction of a will all its provisions must be considered, and the intent of testator, if manifested, must be given effect. . . ."); *In re* Granberry's Estate, 310 So. 2d 708, 711 (Miss. 1975) ("[T]he fundamental rule governing the construction of all wills is to ascertain the intent of the testator"); Waldman v. Hoechst, 487 S.W.2d 541, 542 (Mo. 1972) ("We must determine the intent of the testator from the language of the will if possible. . . .").

346 NetChoice Two-Pager, *supra* note 62.

347 RUFADAA, *supra* note 58, § 7(5)(c).

348 The right to transfer property at death is not without limitations. *See, e.g.*, 2 RESTATEMENT (THIRD) OF PROPERTY: WILLS AND OTHER DONATIVE TRANSFERS § 10.1 cmts. a, c (2003) (describing the general freedom to transfer property at death and limits such as "impermissible racial or other categoric restrictions").

349 PEAC, *supra* note 54, § 1

350 *See* e.g., ALA. CODE § 43-2-834 (2016) (personal representative should proceed "expeditiously"); ARIZ. REV. STAT. ANN. § 14-3703 (2016) (personal representative to act "expeditiously and efficiently as is consistent with the best interests of the estate"); GA. CODE ANN. § 53-7-1 (West 2016) (personal representative has "a general duty to settle the estate as expeditiously and with as little sacrifice of value as is reasonable under all of the circumstances").

to require personal representatives to obtain court orders as a matter of course. Demanding a court order from a personal representative is, more or less, a cost-free way to protect against liability. Indeed, the experiences of Marsha Mehran's father, Justin Ellsworth's father, and Karen Williams suggest that disclosure is not likely to occur without court involvement—each of those examples involved negotiation and court time. Furthermore, a court order pursuant to RUFADAA's requirements, like PEAC's requirements, must include a judicial finding that disclosure does not create liability under federal law.[351] As a result, online service providers are likely to request court orders under RUFADAA because making the demand not only costs them nothing, but also shields them from liability. In short, RUFDAA's requirement that a court order is only necessary 'if requested' will likely transform into a de facto requirement when applied in the real world.

The mandatory court order under PEAC and its analog under RUFADAA are not only cost-free protective mechanisms, but also have the potential to reduce the cumulative financial burden of compliance for online service providers. Whatever it may cost a service provider to acquire and deliver information about an account to a personal representative, the cost is greater than zero. The costs of acquisition and delivery in isolation may not amount to much in the digital age, but presumably an employee of the service provider will have to be involved in the process at some point. And while the costs may be small in an individual case, the financial and opportunity costs could be quite large in the aggregate given the number of online account holders who may seek access and delivery. If the online service provider requires a court order prior to disclosure, however, some access seekers are likely to be dissuaded from the pursuit of a court order that details the specific findings required under either RUFADAA or PEAC. The number of access seekers that opt to forego the court order following a request by an online service provider represents a cost-savings in the aggregate. Much like the legal protection offered by requesting a court order, the potential cost-savings again cause the permissive approach to court orders under RUFADAA to mutate into the mandatory requirement under PEAC.

The mandatory requirement under PEAC and the possible or probable requirement under RUFADAA not only save costs for online service providers, but also add costs to the administration of a testator's estate. As a general matter, an attorney is not required to probate an estate. Probating an estate without the aid of legal counsel, however, can be difficult because of the multiple tasks to be accomplished by a personal representative during estate administration. A personal representative must collect the decedent's assets, identify and pay the decedent's debts, file paperwork with the court such as

351 *See id.*

an inventory, and distribute a decedent's property.[352] Some tasks are straightforward, but others are less than obvious for non-lawyers. For example, state statutes often dictate the order in which a decedent's debts are to be paid.[353] While running afoul of an order of payment statute really only causes problems if the estate cannot retire all of the decedent's debts, most non-estate lawyers, in all likelihood, would not consider the possibility of estate insolvency at the outset of the probate process. Despite its challenges,[354] the intrepid individual is nevertheless perfectly free to tackle the administration of a decedent's estate without the assistance of an attorney.

The factual and legal findings that must be included in court orders under PEAC and RUFADAA, however, all but dictate that a lawyer will be involved in the administration of an account holder's estate. PEAC requires a court to find that "disclosure of the contents is not a violation of 18 U.S.C. § 2701 *et. seq.*, 47 U.S.C. § 222, or other applicable law."[355] Similarly, RUFADAA's possible or probable court orders include a finding that "disclosure of the user's digital assets is reasonably necessary for administration of the estate."[356] Phrases like PEAC's "other applicable law" or RUFADAA's "reasonably necessary" as well as Byzantine references to the United States Code instruct the non-lawyer personal representative to employ an attorney to discover "other applicable law" that might impact disclosure.[357] The down side of court hearings and attorneys, of course, is that they cost money and the estate pays those costs.[358] Paying those costs means that there is less property to be distributed to takers under the will. Although many individuals voluntarily seek legal assistance during estate administration as a routine matter, requiring court orders to disclose digital assets when there is a valid

---

352 *See, e.g.*, COLO. REV. STAT. § 15-12-703 (2016); IND. CODE § 29-1-13-1 (2016); KY. REV. STAT. ANN. § 395.001 (West current through the end of the 2016 regular session); S.C. CODE ANN. 1976 § 62-3-703 (2009 & Supp. 2015); WIS. STAT. § 857.03 (2016).

353 *See, e.g.*, ARK. CODE ANN. § 28-50-106 (West 2016) (payment priority); FLA. STAT. ANN. § 733.707 (West 2016) (order of payment); NEV. REV. STAT. ANN. § 147.195 (West 2015) (priority of payment of debts and charges of estate).

354 Indeed, numerous advice-oriented columns detail the difficulties associated with performing the functions of a personal representative during estate administration. *See e.g.*, Pat Curry, *Estate Executor: No Job for Amateurs*, BANKRATE.COM (Nov. 11, 2002), http://web.archive.org/web/20120308100607/http://www.bankrate.com/brm/news/advice/20021111a.asp; Pamela Yip, *Think Long, Hard Before Becoming Someone's Estate Executor*, DALLAS MORNING NEWS (May 17, 2013), http://www.dallasnews.com/business/personal-finance/headlines/20130517-think-long-and-hard-before-becoming-someones-executor.ece.

355 PEAC, *supra* note 54, § 1(B)(c)(vii).

356 RUFADAA, *supra* note 58, § 8(4)(D)(ii).

357 PEAC, *supra* note 54, § 1(B)(c)(vii) (citing 18 U.S.C. § 2701 *et. seq.* (2012), 47 U.S.C. § 222 (2012)); RUFADAA, *supra* note 58, § 8(4)(D)(ii).

358 *See* e.g., ARK. CODE ANN.§ 28-48-109 (West 2016) (governing repayment of necessary expenses); NEB. REV. STAT. ANN. § 30-2481 (West 2016) (estate litigation expenses); UTAH CODE ANN.§ 75-3-719 (West 2016) (estate litigation expenses).

will that addresses the matter unnecessarily adds to the time and expense of probate to the detriment of the decedent's estate and intent.

Court ordered disclosure that involves lawyers burden all estates that seek access and disclosure, but will be especially onerous for estates that qualify for summary probate. Most states have summary administration procedures for so-called "small estates" that hold property that is valued at less than a designated dollar amount.[359] Although summary procedures vary regarding court and attorney involvement,[360] the basic benefit of summary administration is that it streamlines the probate process by permitting qualifying estates to avoid full, formal probate procedures.[361] In other words, summary procedures reduce probate costs and consume less time.[362] The ubiquity of digital assets and the evidentiary findings required to obtain a court orders under PEAC or RUFADAA, however, all but guarantee that an attorney will be involved in almost all estate proceedings, including those eligible for summary administration. A small estate in Rhode Island, which is defined to be an estate with property valued at $15,000 or less, could be required to obtain a court order for a catalogue or the contents of a digital account.[363] Given the complexity of the evidentiary findings for non-lawyers, a personal representative is likely to retain counsel during administration and the associated costs will be paid from the $15,000 estate. Thus, the mandatory or de facto court orders under PEAC and RUFADAA undercut the procedural benefit of summary administration; requiring court orders drains a small estate of its limited assets, which is contrary to a decedent's intent.[364]

The cost shifting of each model proposal, as well as the legal safe harbor offered therein, suggests a more fundamental critique—the model statutes are aimed at protecting the interests of online service providers at the expense of a testator's intent. If a testator has included a specific provision for access to her digital accounts in a validly executed will,[365] the testator has presumably considered the consequences of divulging the contents of digital accounts

---

359 *See* e.g., CAL. PROB. CODE § 13100 (West 2016) (defining small estates as those less than $150,000); OKLA. STAT. tit. 58, § 241 (2016) (designating small estates as those less than $150,000).

360 Joseph N. Blumberg, *51 Flavors: A Survey of Small Estate Procedures Across the Country*, 28 PROB. & PROP., 31, 32 (JULY-AUG. 2014) (distinguishing between the small estate process that requires court involvement and that which does not require any court oversight).

361 *Id.*

362 *Id.* at 33 ("A full probate proceeding typically lasts at least six months, and often years. Summary Administration, particularly in a state that requires publication, commonly lasts at least six months. Summary Administration reduces the courts' dockets compared to full probate proceedings, but only the Affidavit Procedure takes those cases out of the court system altogether."); *see also id.* (noting that some state statutes require an attorney).

363 R.I. GEN. LAWS § 33-24-1 (2016).

364 The word "small" as it applies to "small estates" is relative. One might argue that Oklahoma's designation of estates that contain property valued at $150,000 or less does not qualify as a "small" estate.

365 The phrase "specific provision" is used to avoid an issue regarding access based upon broad language in a will's residuary clause.

and chosen to make the contents available for distribution. Under those circumstances, a testator's explicit expression of consent to access to and disclosure of the contents of digital accounts in a will represents the testator's deliberate waiver of the protection offered by the recognition of posthumous privacy. In fact, the inclusion of a will provision waiving posthumous privacy cannot be anything but the result of due deliberation—the issue is too novel and too sparsely included in existing wills for any waiver provision to be considered boilerplate and therefore not the product of considered decision-making for the ordinary testator. A testator's specific intent to permit access and disclosure should not be re-examined by a court for the purpose of obtaining a court order to command what the testator has already commanded by an explicit provision in a will.

If the drafters of RUFADAA and PEAC actually sought to respect an account holder's posthumous privacy designations, the language of each model statute should mandate disclosure if a testator intends to disclose the contents of an account. To obtain access and disclosure, a personal representative could be required to produce a death certificate, appropriate account identification, letters testamentary or a small estate affidavit, and the will with an explicit direction regarding disclosure.[366] Granting disclosure of desired information following reception of those instruments would bring post-mortem access in line with other assets held by third parties after the death of an account holder. Banks, for example, may release funds in a decedent's bank accounts after receiving a death certificate, information that identifies the account, and letters testamentary or a small estate affidavit in the appropriate case.[367] Similarly, state statutes provide personal representatives with access to a decedent's safe deposit box without a court order.[368] Providing access and disclosure without court involvement for an account holder who leaves a validly executed will puts the account holder in full control of account contents after death and reflects a firm commitment to honoring the intent of a deceased account holder.

Reducing the potential for court involvement in the decision to access and disclose information stored in digital assets does not mean that there is no role for a court to play under all circumstances. To the contrary, a court order could be requested in good faith to establish the validity of the authority of the personal representative if a will is unclear, to interpret ambiguous language appearing to grant access to digital accounts, or to clarify the identity of the account or the account holder. In those instances, online service providers must have a way to determine the legal veracity of the request for an

366 A correspondent with information remaining in a decedent's account could retain the right to object to the disclosure of information in which correspondent had an interest.

367 *See, e.g., How to Notify Bank of America When a Customer Passes Away*, BANK OF AM., https://www.bankofamerica.com/help/help-when-a-customer-passes-away.go (last visited Aug. 31, 2016).

368 *See e.g.*, IND. CODE § 29-1-13-1.5 (2016); N.C. GEN. STAT. ANN. § 28A-15-13 (2016); TEX. EST. CODE ANN. § 151.003 (West 2015).

account record or contents. Indeed, transferring account information in the absence of a court order amidst legal uncertainty would be injudicious because of the risk of liability under state or federal law for wrongful disclosure. Moreover, providing a mechanism to ensure the legality of a request as a safety measure does not contravene a decedent's intent for access to and disclosure of account contents. Where resort to court is necessary, a question exists about whether the decedent's intent is being fulfilled or what the decedent intended by the language in the will; court involvement in such cases protects a decedent's intent to the extent it can be deciphered.

In some cases, honoring a testator's intent as expressed on the face of the will could have a deleterious effect on administration. A testator, for example, could instruct that no one is to access an email account after death for any reason and that intent should generally be honored. But if a personal representative cannot account for all of the decedent's assets or debts, a possibility exists that evidence of either could be stored in the email account. Under those circumstances, the testator's intent to bar posthumous access to the digital information frustrates the process of administering the estate. In economic terms, the intent to bar access creates externalities that burden personal representatives and the takers under the will who may have to wait for distribution of estate property. Instances where a personal representative finds herself facing uncertainty about the existence of assets or debts might be rare, but they are not inconceivable. Indeed, the impetus for Connecticut's first generation statute involved a surviving spouse who needed to access a decedent spouse's email account for business purposes.[369] In cases where information cannot be obtained without access, the costs of posthumous privacy exceed its benefits; a testator's intent cannot be satisfied regardless of its consequences.

Rather than complete immunity from access and disclosure based upon testator's will, model statutes like RUFADAA and PEAC should account for the possibility that a testator's intent for posthumous privacy may need to be breached to promote the orderly administration of estates. In fact, two of the present provisions in each of the statutes could form the foundation for obtaining a record of communications or disclosure of contents if needed during estate settlement despite a testator's expressed intent for nondisclosure. RUFADAA §7(5)(C)(iv) requires a court to find that disclosure is "reasonably necessary for administration of the estate."[370] Similarly, PEAC requires a court to find that a request for access is "narrowly tailored to effect the purpose of administration of the estate."[371] To satisfy either standard, a personal representative could identify the information needed, explain its necessity, and describe the failed steps taken to procure the information without access to account information. All of the evidence necessary to satisfy each of those elements should be readily available to the personal representative without

369 *See supra* notes 70–75 and accompanying text.

370 RUFADAA, *supra* note 58, § 7(5)(C)(iv).

371 PEAC, *supra* note 54, § 1(A)(f).

the cost of discovery. A testator's intent for posthumous privacy should be respected, but a testator's intended privacy cannot be an insurmountable barrier that stymies estate administration.

CONCLUSION

Within the past year, a flurry of legislative activity has orbited what was a straightforward issue not long ago in the non-digital world – access to and disclosure of property in a decedent's estate. For some, the issue of post-mortem access is cut and dry because information stored in digital assets is a decedent's property just like postal mail, handwritten notes, or any other tangible property in a decedent's home. Information stored in digital assets may be deemed "property" of a decedent, but it is different from property in the tangible world. Digital information can remain available for a long time after the death of the account holder; one's online information may create a sort of immortality for the account holder. Furthermore, the sheer volume and storage capability in the modern digital age has no analog in the past. To that end, Chief Justice Roberts observed in *Riley v. California*[372] that a cell phone may store "a broad array of private information never found in a home in any form."[373] Justice Alito echoed a similar refrain by noting that a cell phone is "capable of storing and accessing a quantity of information, some highly personal, that no person ever would have had on his person or in hard-copy form."[374] Indeed, the problems associated with post-mortem access to digital assets during estate administration would not have captured widespread legislative interest if digital property was the exact equivalent of tangible property—the issue would have been readily addressed by settled law.

The quantity, capability, and durability of digital information not only pressures the law of wills, but also challenges the traditional view that individual privacy ends at death. But unlike the staid law of wills, the law of privacy has not been a static concept from an historical perspective. To that end, the influential article, *The Right of Privacy* by Warren and Brandeis, maintained that "recent inventions" justified the development of a principle that protected one's right "to be let alone" and stitched existing legal doctrines together to create a concept denominated as a "right of privacy."[375] Indeed, statutory exceptions to the termination of an individual's interest in

---

372 134 S.Ct. 2473 (2014)

373 *Id.*

374 *Id.* at 2496 (Alito, J., concurring). For more on the differences between digital and physical assets, *see* e.g., Lange, supra note 252 ("[D]igital assets differ significantly from physical estates. . . .").

375 Samuel D. Warren and Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 195 (1890) ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.'") (quoting THOMAS M. COOLEY, LAW OF TORTS 29 (1880))); *id.* at 197 ("It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.").

privacy at death illustrate privacy's modern malleability. Within the context of post-mortem access to digital assets, the inability to protect posthumous privacy by employing the protective approaches of statutory exceptions like HIPPA and FOIA warrants the inclusion of posthumous privacy among the factors to be considered when crafting a legislative response. Once included in the legislative balance, the weight of a decedent's interest in privacy tips the privacy scale toward non-disclosure for individuals who die intestate and toward disclosure if a testator has instructed that account contents be available in a will. Doing so most closely conforms to the fundamental law of wills—honoring a decedent's intent.