

The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property

JAMES D. LAMM, CHRISTINA L. KUNZ, DAMIEN A. RIEHL
& PETER JOHN RADEMACHER¹

I.	INTRODUCTION	385	R
II.	DIGITAL PROPERTY: INTANGIBLE, BUT IMPORTANT	388	R
	A. <i>What Is Digital Property?</i>	388	R
	B. <i>Why Digital Property Should Not Be Overlooked</i>	389	R
	1. FINANCIAL VALUE	389	R
	2. SENTIMENTAL VALUE	390	R
III.	FOUR FIDUCIARIES AND A LOT OF PROBLEMS	391	R
	A. <i>Four Bodies of Fiduciary Law Facing Similar Concerns</i>	391	R
	1. BASIC STRUCTURE OF STATUTORY POWER OF ATTORNEY	391	R
	2. BASIC STRUCTURE OF CONSERVATORSHIP	393	R
	3. BASIC STRUCTURE OF PROBATE ADMINISTRATION	394	R
	4. BASIC STRUCTURE OF TRUSTS	396	R
	B. <i>Presenting the Problems</i>	397	R
	1. RESTRICTIONS ON ACCOUNT HOLDERS	399	R
	2. RESTRICTIONS ON THE FIDUCIARIES	399	R
	3. RESTRICTIONS ON DIGITAL SERVICE PROVIDERS	403	R
IV.	PURPORTED SOLUTIONS AND THEIR SHORTCOMINGS	406	R
	A. <i>Private Entities Promoting Private or Commercial Planning Strategies</i> ..	406	R
	B. <i>State Protection of Fiduciaries in Digital Property Management</i>	411	R
V.	A HOLISTIC APPROACH TO RESOLUTION	412	R
	A. <i>Congressional Amendments</i>	413	R
	B. <i>Uniform State Law</i>	414	R
	C. <i>Best Practices in the Interim</i>	416	R
	1. HOW ACCOUNT HOLDERS SHOULD PLAN FOR DEATH OR INCAPACITY ..	416	R
	2. HOW FIDUCIARIES SHOULD MANAGE PROPERTY WHEN NO PLAN		
	EXISTS	419	R
VI.	CONCLUSION	420	R

I. INTRODUCTION

The digital world is a popular place these days. In its fourth quarter of 2012, Facebook reported 618 million daily users.² In fiscal year 2012, Google reported 235 million active users across its properties (e.g.,

1. James D. Lamm is a Principal at Gray Plant Mooty in Minneapolis, Minnesota. Christina L. Kunz is a Professor Emerita at William Mitchell College of Law in Saint Paul, Minnesota. Damien A. Riehl is an Associate at Robins, Kaplan, Miller & Ciresi in Minneapolis, Minnesota. Peter John Rademacher is a law student at William Mitchell College of Law in Saint Paul, Minnesota, and will receive his Juris Doctor in May 2014.

2. *Investor Relations: Facebook Reports Fourth Quarter and Full Year 2012 Results*, FACEBOOK (Jan. 30, 2013), <http://investor.fb.com/releasedetail.cfm?ReleaseID=736911>.

Gmail and YouTube)³; Activision Blizzard estimated over 9.6 million subscribers to World of Warcraft⁴; and the list goes on.⁵ The United States's Internet use ranks among the highest—both in number and percentage of population.⁶ Members, users, and subscribers (“account holders”) accumulate digital property by uploading photographs, videos, and other data, investing time into profile development, adding written material, and building their own subscribership accounts.

How should this property be managed during the account holders' lives? Upon the account holders' deaths, what should happen to it? How should it be maintained? How should it be distributed? As one author notes, “[M]ore and more of what happens in the [physical] world is also seeping into the [digital] world”⁷ That includes our need for fiduciaries in many aspects of life and death. Every single Internet user will die, many will suffer some form of incapacity, and some will have valuable or significant digital property that needs to be protected and managed.⁸ In the physical world, legal mechanisms can address these issues.⁹

3. Google Inc., Annual Report (Form 10-K), 3 (Jan. 29, 2013), available at <http://www.sec.gov/Archives/edgar/data/1288776/000119312513028362/d452134d10k.htm>.

4. Press Release, Activision Blizzard, Activision Blizzard Announces Better-Than-Expected Fourth Quarter & Calendar Year 2012 Results (Feb. 7, 2013) (on file with author), available at http://files.shareholder.com/downloads/ACTI/2329417148x0x634081/fbb6a75d-f965-442b-8d6a-bde335918118/Q4_2012_atvi_press_release.pdf.

5. Yahoo! Mail is reported to have over 281 million unique visitors. Rani Molla, *Gmail Finally Beats Hotmail, According to Third-Party Data [Chart]*, GIGAOM (Oct. 31, 2012, 10:38 AM), <http://gigaom.com/2012/10/31/gmail-finally-beats-hotmail-according-to-third-party-data-chart/> (place cursor on blue graph bar representing Yahoo! Mail worldwide e-mail ranking). Twitter is reported at over 170 million active users. Ingrid Lunden, *Twitter May Have 500M+ Users but Only 170M Are Active, 75% on Twitter's Own Clients*, TECHCRUNCH (July 31, 2012), <http://techcrunch.com/2012/07/31/twitter-may-have-500m-users-but-only-170m-are-active-75-on-twiters-own-clients/>. PayPal is reported at over 117 million users. Ryan Kim, *PayPal Launches Pre-Paid Cards to Help Cash Lovers Buy Online*, GIGAOM (Dec. 13, 2012, 8:49 AM), <http://gigaom.com/2012/12/13/paypal-launches-pre-paid-cards-to-help-cash-lovers-buy-online/>.

Soundcloud operates with roughly 200 million monthly users, Tumblr with 216 million monthly visitors, and Wordpress hosts over 66 million blogs. Craig Smith, *How Many People Use the Top Social Media, Apps & Services? (September 2013)*, DIGITAL MARKETING RAMBLINGS (Sept. 2, 2013), <http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/3/>.

6. *Top 20 Internet Countries by Users—2012 Q2*, INTERNET WORLD STATS, <http://www.internetworldstats.com/top20.htm> (last updated Mar. 6, 2013).

7. Mathew Ingram, *Facebook and Death: Blurring the Line Between the Real and Virtual*, GIGAOM (Nov. 13, 2012, 2:09 PM), <http://gigaom.com/2012/11/13/facebook-and-death-blurring-the-line-between-the-real-and-virtual/>.

8. In 2008, the European Network and Information Security Agency estimated that “the real money value of virtual world objects being traded each year [was] \$2 billion.” Simon Hill, *Most Expensive Items Ever Sold in an MMO*, ALTERED GAMER, <http://world-of-warcraft.alteredgamer.com/wow-other-items/29070-most-expensive-items-ever-sold-in-an-mmo/> (last updated Apr. 18, 2012).

9. See generally, e.g., UNIF. GUARDIANSHIP AND PROTECTIVE PROCEEDINGS ACT (1998);

Other bodies of law do not impede these mechanisms, which have evolved over hundreds of years, but the digital world is like the “Wild West,” in that its growth has outpaced legal and regulatory efforts.¹⁰ Although federal and state governments have enacted laws to control aspects of the digital world, some of these laws predate the World Wide Web¹¹ and stand as inadvertent barriers to the execution of fiduciary duties in the digital world. State legislatures, private entities, and courts have made some efforts to correct these problems, but no current solutions provide the level of certainty that account holders and courts typically seek in fiduciary property management. Consequently, account holders are uncertain about the future of their digital property; fiduciaries must choose between refusing to manage digital property at the risk of civil liability, and executing their duties at the risk of criminal liability. Additionally, digital service providers (“service providers”) must fend for themselves by carefully crafting their terms of service (“TOS”) and privacy policies (“PPs”).

This article discusses four types of fiduciaries, each of which is affected by the vast growth in and the need to manage digital property. The article begins by defining digital property and discussing why it must be managed.¹² The article then discusses how digital property affects powers of attorney, conservatorships, probate administration, and trusts.¹³

After illustrating the problems that digital property creates for each fiduciary, the article shifts to resolving these problems. It begins by debunking purported solutions by both private and governmental entities.¹⁴ It concludes by offering a holistic approach to resolving the conflicts facing account holders, fiduciaries, and service providers and providing the level of security sought in fiduciary property management, as well as a best-practices approach in the interim to a complete

UNIF. POWER OF ATTORNEY ACT (2006); UNIF. PROBATE CODE (amended 2010); UNIF. TRUST CODE (amended 2010).

10. E.g., Michael B. Sapherstein, *Intelligent Agents and Copyright: Internet Technology Outpaces the Law . . . Again*, B.C. INTELL. PROP. & TECH. F. (Oct. 28, 1997), <http://bciprf.org/wp-content/uploads/2011/07/56-INTELLIGENT-AGENTS-AND-COPYRIGHT.pdf> (generally noting legislation’s inherent inability to catch up with technology’s fast pace).

11. In 1986, Congress enacted the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified at 18 U.S.C § 1030 (2012)); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510-2522, 2701-2712 (2012)). The World Wide Web was introduced in 1990. Tim Berners-Lee, *Pre-W3C Web and Internet Background*, W3C, <http://www.w3.org/2004/Talks/w3c10-HowItAllStarted/?n=15> (last visited Sept. 7, 2013).

12. See *infra* Part II.

13. See *infra* Part III.

14. See *infra* Part IV.

solution.¹⁵

II. DIGITAL PROPERTY: INTANGIBLE, BUT IMPORTANT

The term “property” has many definitions. When used in the context of fiduciary management, property generally “includes both real and personal property or any interest therein and means anything that may be the subject of ownership.”¹⁶ But what is digital property, and why should anyone care? This section sheds light on the nature of digital property, what it includes, and why it is important.

A. *What Is Digital Property?*

Personal property can be tangible or intangible. Whereas tangible personal property takes corporeal form,¹⁷ intangible personal property lacks physical existence.¹⁸ Intangible personal property includes financial accounts, stocks, options, intellectual property rights, and so-called digital property.¹⁹ One type of digital property is electronically stored information, which may be stored locally or “in the cloud.” While digital property can take the form of Web sites, such as “e-mail, social networking sites (Facebook, LinkedIn, Google+, MySpace, etc.), eBay, PayPal, Web pages, blogs, photo sharing accounts like Flickr, video sharing accounts like YouTube, music accounts like iTunes and Pandora, online video games like World of Warcraft, [and] online storage accounts,”²⁰ most service providers deliver these Web site accounts as a service without vesting any property rights in the subscribers.²¹ The TOS may prevent an account holder from transferring the account itself or allowing others to access the account.²²

More commonly, individuals’ digital property is the content they upload onto these Web sites. For instance, when account holders post

15. See *infra* Part V.

16. UNIF. PROBATE CODE § 1-201(38) (amended 2010); see UNIF. POWER OF ATTORNEY ACT § 102(10) (2006) (providing an equivalent definition).

17. See BLACK’S LAW DICTIONARY 1337–38 (9th ed. 2009).

18. *Id.* at 1336.

19. See, e.g., Jason Mazzone, *Facebook’s Afterlife*, 90 N.C. L. REV. 1643, 1648 (2012); Rex M. Anderson, *Digital Assets in Estates*, ARIZ. ATT’Y, Mar. 2013, at 44, 44.

20. James D. Lamm, *Digital Death: Estate Planning for Passwords, Online Accounts, and Digital Property 2* (Jan. 20, 2012), available at http://www.actec.org/Documents/misc/James_Lamm_-_Digital_Death_01_20_2012.pdf.

21. See, e.g., *World of Warcraft Terms of Use*, BLIZZARD ENTERTAINMENT, http://us.blizzard.com/en-us/company/legal/wow_tou.html (last updated Aug. 22, 2012) (granting the user “a Limited License to Use the Service”).

22. For a clear discussion of the difference between accounts and content in accounts, see Jim Lamm, *What Happens to Your Apple iTunes Music, Videos, and eBooks When You Die?*, DIGITAL PASSING (Sept. 4, 2012), <http://www.digitalpassing.com/2012/09/04/apple-itunes-music-videos-ebooks-die/>.

songs, photos, videos, and other data, these items qualify as digital property.²³ Digital property rights may also exist for subscribers to online games, such as Farmville, Second Life, and World of Warcraft, where subscribers have paid for and may have even created or acquired online gaming avatars and other assets in online games.²⁴ Moreover, digital property can include intellectual property, such as copyrights, trademarks, trade secrets, rights of privacy, rights of publicity, and the like.²⁵ Take copyright, for instance. “Copyright protection subsists, in accordance with this title, in original works of authorship *fixed in any tangible medium of expression . . .*”²⁶ “A work is ‘fixed’ in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.”²⁷ Copyrights often vest in account holders—regardless of where their content is posted or stored, and regardless of whether the medium is digital or analog—because they are the authors.²⁸

This article focuses on an account holder’s digital property rights or intellectual property rights in the account contents that are stored by a service provider and accessed through a service provider’s Web site or other communications protocol. This article does not cover a service provider’s service contracts to use its hardware, software, Web site, or other services.

B. *Why Digital Property Should Not Be Overlooked*

The United States Department of Commerce reported from census data that from 2000 to 2010, the percentage of Internet-connected households jumped from 41.5% to 71.1%.²⁹ From domain names to blogs, avatars to social media, this rising tide of Internet use translates into more digital property that can have both financial and sentimental value.

1. FINANCIAL VALUE

A 2011 survey found that U.S. consumers valued their digital

23. *See id.*

24. *See infra* Part II.B.1.

25. *See generally* Pamela Samuelson, *Digital Media and the Changing Face of Intellectual Property Law*, 16 RUTGERS COMPUTER & TECH. L.J. 323 (1990) (discussing the legal challenges posed by developing digital media).

26. 17 U.S.C. § 102(a) (2012) (emphasis added).

27. *Id.* § 101.

28. *See id.* § 201(a).

29. NAT’L TELECOMMS. & INFO. ADMIN., U.S. DEP’T OF COMMERCE, DIGITAL NATION: EXPANDING INTERNET USAGE 7 fig.1 (2011), *available at* http://www.ntia.doc.gov/files/ntia/publications/ntia_internet_use_report_february_2011.pdf.

assets, stored across multiple digital devices, at an average of \$55,000 per person.³⁰ That value can emanate from intellectual property rights, advertising revenue from Web sites and blogs, avatar development, virtual property in virtual worlds, and domain names.³¹ While much digital property has little or no financial value, some items have considerable value. Many, but not all, examples of valuable digital property come from the gaming and virtual-world communities. For instance, in a single transaction in 2005, Jon Jacobs mortgaged his home to purchase a virtual resort for \$100,000 in real money³²; in 2011, that same resort's estimated value was \$1 million.³³ In 2011, a man paid \$16,000 for a digital sword to be used in a game that would not be released until the spring of 2012.³⁴ In 2012, Blizzard opened an auction house, where players could exchange real money for digital gear.³⁵ In the same year, an investor purchased land deeds in Planet Calypso for \$2.5 million.³⁶ Today, World of Warcraft players pay approximately \$15 for 1,000 "gold"—currency for the game.³⁷ Outside of the gaming and virtual-world realms, the digital world even houses a decentralized digital currency called Bitcoin, which is created through the process of "mining" and can be exchanged for nationally recognized currencies.³⁸ In July 2013, one Bitcoin equated to \$76.75.³⁹

2. SENTIMENTAL VALUE

Some digitally stored photographs, poems, messages, videos, e-mails, and the like may have sentimental (rather than financial) value to

30. McAfee Reveals Average Internet User Has More Than \$37,000 in Underprotected "Digital Assets", MCAFEE (Sept. 27, 2011), <http://www.mcafee.com/us/about/news/2011/q3/20110927-01.aspx>.

31. Lamm, *supra* note 20, at 2.

32. E.g., Oliver Chiang, *Meet the Man Who Just Made a Half Million from the Sale of Virtual Property*, FORBES (Nov. 13, 2010, 7:20 PM), <http://www.forbes.com/sites/oliverchiang/2010/11/13/meet-the-man-who-just-made-a-cool-half-million-from-the-sale-of-virtual-property/>.

33. Hill, *supra* note 8.

34. Jim Sterling, *Man Buys Virtual Sword for Unreleased Game, Pays \$16,000*, DESTRUCTOID, (Dec. 29, 2011, 1:00 PM), <http://www.destructoid.com/man-buys-virtual-sword-for-unreleased-game-pays-16-000-218682.phtml>.

35. Paul Tassi, *Why Diablo 3's Real Money Auction House Should Not Be Your Summer Job*, FORBES (June 13, 2012, 10:04 AM), <http://www.forbes.com/sites/insertcoin/2012/06/13/why-diablo-3s-real-money-auction-house-should-not-be-your-summer-job-2/>.

36. Press Release, MindArk, Entropia Universe Receives \$2.5 Million Dollars from One Investor in Planet Calypso Citizenship System (Apr. 4, 2012), *available at* <http://www.prnewswire.com/news-releases/entropia-universe-receives-25-million-dollars-from-one-investor-in-planet-calypso-citizenship-system-146075785.html>.

37. Hill, *supra* note 8.

38. See Leah Yamshon, *Portrait of a Bitcoin Miner: How One Man Made \$192K in Virtual Currency*, IT WORLD (July 10, 2013, 1:11 PM), <http://www.itworld.com/internet/364484/portrait-bitcoin-miner-how-one-man-made-192k-virtual-currency>.

39. *Id.*

R

R

R

members, users, or subscribers—as well as their families and friends.⁴⁰ As one commentator noted, “[P]ostings . . . might be of value given what could be done with digital data in the future. . . . On the horizon may be interactive holograms that look and sound like a deceased individual, based upon that individual’s digital archive”⁴¹ Even if interactive holograms never come to fruition, more and more memorabilia is stored digitally, replacing an outmoded system of physical storage.⁴² Therefore, there is still good reason to protect and manage certain digital property, even if it has no financial value.

III. FOUR FIDUCIARIES AND A LOT OF PROBLEMS

A fiduciary ensures that property is well managed, during the life or after the death of the property owner. In the physical world, the fiduciary’s roles are widely accommodated by other bodies of law (such as contract law, banking and payments law, privacy law, criminal law, and the like). But the same cannot be said for the digital world, which has developed without close attention to fiduciaries’ roles.⁴³ This section briefly describes power of attorney, conservatorship, probate administration, and trusts⁴⁴—as well as why digital property poses problems for each.⁴⁵

A. *Four Bodies of Fiduciary Law Facing Similar Concerns*

1. BASIC STRUCTURE OF STATUTORY POWER OF ATTORNEY

Under the Uniform Power of Attorney Act of 2006, an agent is “a person granted authority to act for a principal”⁴⁶ The principal⁴⁷ generally grants that authority by executing and signing (or consciously witnessing the signature of) a power of attorney.⁴⁸ An agent, once granted authority, may accept appointment by exercising authority as an

40. See Lamm, *supra* note 20, at 4–5.

41. Mazzone, *supra* note 19, at 1650–51.

42. See Lamm, *supra* note 20, at 5.

43. Cf. Stephen J. Lusch, *State Taxation of Cloud Computing*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 369, 371 (2013) (“As the digital environment in which we live continues to change at speeds that were unfathomable two decades ago, archaic state tax systems have struggled to keep pace.”).

44. See *infra* Part III.A. To avoid unnecessary discussion of jurisdictional splits, this article relies solely on the Uniform Power of Attorney Act, the Uniform Guardianship and Protective Proceedings Act, the Uniform Probate Code, and the Uniform Trust Code to explain their respective bodies of law.

45. See *infra* Parts III.B–C.

46. UNIF. POWER OF ATTORNEY ACT § 102(1) (2006). The Uniform Power of Attorney Act replaced the term “attorney in fact” with “agent,” as a means of alleviating confusion among laypeople between an “attorney in fact” and an “attorney at law.” *Id.* § 102 cmt.

47. *Id.* § 102(9).

48. *Id.* § 105.

agent, by performing duties as an agent, or by indicating acceptance through assertions or conduct.⁴⁹

When a power of attorney becomes effective, the agent receives the general authority referenced in the power of attorney,⁵⁰ incidental authority that accompanies all general authority granted,⁵¹ and additional authority expressly granted through special instructions in the power of attorney.⁵² These authorities include the power to manage the specified subject matters, including property,⁵³ and the cumulative effect of these authorities can be narrow or substantial.

Although an agent generally has no initial duty to act, if he or she does take action, he or she must adhere to certain duties, “[n]otwithstanding provisions in the power of attorney.”⁵⁴ Those duties include acting in accordance with the principal’s reasonable expectations, or, if unknown, in the principal’s best interest and acting in good faith.⁵⁵ In addition to these mandatory standards, unless otherwise provided in a power of attorney, an agent must act to avoid conflicts of interest that would impair his or her ability to act impartially for the principal’s best interests and must seek to maintain the principal’s estate plan, taking into consideration the nature and value of property and the likelihood of obligations and need for maintenance.⁵⁶ Finally, if an agent is selected for his or her special skills, he or she must apply those skills in the execution of his or her duties.⁵⁷

If the agent violates the power of attorney or its accompanying duties, a court may grant damages to restore the value of the principal’s property and reimburse the principal for attorney’s fees paid on behalf of the agent.⁵⁸ However, courts are not restricted from awarding other forms of relief provided for by other laws of the governing jurisdiction.⁵⁹ To ensure the likely enforcement of an agent’s duties, there are “broad categories of persons who have standing to petition the court for . . . review of the agent’s conduct,”⁶⁰ including a “person that dem-

49. *Id.* § 113.

50. *Id.* § 202 (providing general authority for subject matter listed in Sections 204 through 217 that is referenced in an executed power of attorney).

51. *Id.* § 203 cmt.

52. *Id.* § 201, 201 cmt.

53. *See, e.g., id.* §§ 203, 205, 208–09.

54. *Id.* § 114(a); *see also id.* § 113 cmt.

55. *Id.* § 114(a)(1)–(2).

56. *Id.* § 114(b)(2), (6).

57. *See id.* § 114(e) (providing that courts must consider an agent’s special skills when evaluating the agent’s care, competence, and diligence).

58. *Id.* § 117.

59. *Id.* § 123, 123 cmt.

60. *Id.* § 116 cmt.

onstrates sufficient interest in the principal's welfare."⁶¹

2. BASIC STRUCTURE OF CONSERVATORSHIP

Under the Uniform Guardianship and Protective Proceedings Act of 1998, a conservator is "a person who is appointed by a court to manage the estate of a protected person."⁶² A court can appoint a conservator upon the petition of:

- (1) the person to be protected;
- (2) an individual interested in the estate, affairs, or welfare of the person to be protected . . . ; or
- (3) a person who would be adversely affected by lack of effective management of the property . . . of the person to be protected.⁶³

After ascertaining that the person to be protected lacks the ability to manage his or her own property or business affairs or has property that will otherwise be wasted,⁶⁴ a court may appoint a conservator.⁶⁵ Once appointed, a conservator can accept the office by filing an acceptance of appointment and submitting any required bond, after which the court will issue letters of conservatorship.⁶⁶

When a conservatorship becomes effective, a conservator typically has all available authority unless expressly limited in the court order and on the letters of conservatorship.⁶⁷ The conservator has authority over most aspects of property management,⁶⁸ distribution and expenditures for the care of the protected person and his or her dependents,⁶⁹ and management of the protected person's estate plan subject to court approval.⁷⁰ Essentially, a conservator obtains complete managerial authority over the protected person's property at least to the extent that the protected person is unable to manage his or her property.

A conservator's acts are constrained by certain duties. A conservator must "observe the standards of care applicable to a trustee";⁷¹ refrain from any exercise of authority that is unnecessary;⁷² develop a plan that is "based on the actual needs of the person [to be protected] and take into consideration the best interest of [that] person";⁷³ and take into

61. *Id.* § 116(a)(8).

62. UNIF. GUARDIANSHIP & PROTECTIVE PROCEEDINGS ACT § 102(2) (1998).

63. *Id.* § 403(a).

64. *See id.* § 401(2).

65. *Id.* § 409(a)–(b).

66. *Id.* § 110.

67. *Id.* § 425(a).

68. *Id.* § 425(b).

69. *Id.* § 427(a).

70. *Id.* § 411(a).

71. *Id.* § 418(a).

72. *Id.* § 418(b).

73. *Id.* § 418(c).

account any known estate plan of the protected person when making decisions regarding investment, distribution, and powers of revocation.⁷⁴

“[A] court may require a conservator to furnish a bond conditioned upon faithful discharge of all duties of the conservatorship according to law, with sureties as it may specify.”⁷⁵ The court can then supervise the conservator’s execution of the conservatorship.⁷⁶ Any interested person may bring a proceeding against the surety for the conservator’s breach of the obligation secured by the bond.⁷⁷ The court may hear proceedings against the bond until the bond is exhausted.⁷⁸ In addition to the conservator’s liability under the bond, the protected person, or a person interested in the protected person’s welfare, may petition the court to terminate the conservator’s appointment under the standard of “the best interest of the . . . protected person.”⁷⁹

3. BASIC STRUCTURE OF PROBATE ADMINISTRATION

Under the Uniform Probate Code of 2010, a personal representative can be an executor (named in a valid will) or an administrator (appointed in the absence of a valid will).⁸⁰ For the personal representative to be appointed, he or she must petition the court or Registrar⁸¹ (this article will refer only to the court), at which time the court may make such an appointment.⁸² A personal representative may then choose to accept office by filing “any required bond and a statement of acceptance of the duties of the office.”⁸³ After the filing, the court will issue letters for the estate’s administration.⁸⁴

The personal representative has power over the decedent’s estate equivalent to what “an absolute owner would have.”⁸⁵ Except as restricted by a will or an order in a formal proceeding, a personal representative must act “for the benefit of the interested persons” and has a range of powers, including the following: (1) retaining assets; (2) receiving assets; (3) depositing or investing liquid assets of the estate; (4) acquiring or disposing of assets; and (5) abandoning property that is

74. *Id.* § 418(d).

75. *Id.* § 415.

76. *See, e.g., id.* § 419(a) (requiring the conservator to prepare an inventory of the estate); *id.* § 420(a) (requiring the conservator to report to the court annually, unless otherwise directed).

77. *Id.* § 416(a)(3).

78. *Id.* § 416(a)(4).

79. *Id.* § 112(b).

80. UNIF. PROBATE CODE § 1-201(35) (amended 2010).

81. *Id.* § 3-402(a)–(b) (formal testacy); *id.* § 3-301(a) (informal probate).

82. *Id.* § 3-103.

83. *Id.* § 3-601.

84. *See id.* § 3-103.

85. *Id.* § 3-711.

valueless.⁸⁶ However, unlike a conservator, a personal representative's power is not accompanied by vesting of title.⁸⁷ The delegation of power without title serves to "ease[] the succession of assets which are not possessed by the personal representative."⁸⁸

A personal representative must pursue a very specific end: to settle and distribute the decedent's estate.⁸⁹ This task must be performed in compliance with the will, any court orders, and the statutory obligations to "observe the standards of care applicable to trustees" and execute tasks "as expeditiously and efficiently as is consistent with the best interests of the estate," as well as those of any successors.⁹⁰

Because of the high stakes in the context of probate administration, the court remains involved and has power to ensure that the estate's administration is carried out properly. Under informal proceedings, the court may require a bond "upon appointment of a special administrator" or when a will expressly requires a bond.⁹¹ In formal proceedings, the court may require a bond unless a will expressly relieves the personal representative of the bond requirement.⁹² Additionally, an interested party may always demand a bond, so long as the party's interest is sufficient and the court finds the bond desirable.⁹³ During administration of the estate, any interested person may petition the court to bring proceedings against the bond for the personal representative's failure to meet his or her fiduciary obligations.⁹⁴ The bond may be proceeded against until exhausted.⁹⁵

In addition to an action against the personal representative's bond, an interested person may petition the court to temporarily restrain the personal representative from specified actions that "would jeopardize unreasonably the interest of the applicant or of some other interested person."⁹⁶ Finally, any interested person may petition the court to permanently remove a personal representative for cause,⁹⁷ which the court will find in any of the following instances: (1) removal would be in the best interest of the estate; or (2) "the personal representative has disregarded an order of the court, . . . mismanaged the estate, or failed to

86. *Id.* § 3-715 (1)–(2), (5)–(6), (11).

87. *Id.* § 3-711 cmt.

88. *Id.*

89. *Id.* § 3-703(a).

90. *Id.*

91. *Id.* § 3-603.

92. *Id.*

93. *Id.* § 3-605. The 2010 Uniform Probate Code sets the threshold interest at \$5,000. *Id.*

94. *Id.* § 3-606(a)(4).

95. *Id.* § 3-605(a)(5).

96. *Id.* § 3-607(a).

97. *Id.* § 3-611(a).

perform any duty pertaining to the office.”⁹⁸

4. BASIC STRUCTURE OF TRUSTS

Under the Uniform Trust Code of 2010, a trustee can be “[a]ny natural person . . . [that] has capacity to hold title to property free of trust.”⁹⁹ When appointed, a trustee has the authority to act for the settlor.¹⁰⁰ The settlor grants that authority by creating a trust and transferring property to the trustee either in the present or the future through some trigger.¹⁰¹ Once granted authority, a trustee may accept the trusteeship “by [either] substantially complying with a method of acceptance provided in the terms of the trust; or . . . if the terms of the trust do not provide a method or the method provided in the terms is not expressly made exclusive,” by other means of indicating acceptance.¹⁰² The trustee must then submit any required bond.¹⁰³

When a trust becomes effective, the trustee obtains certain powers over the trust and trust property. These powers include the powers conferred by the trust instrument;¹⁰⁴ the power of an unmarried, competent, individual owner, except as limited by the trust;¹⁰⁵ the powers appropriate to properly manage and distribute trust property;¹⁰⁶ the power to collect trust property;¹⁰⁷ and the power to manage the trust property through various transactions with beneficiaries or third parties.¹⁰⁸ In addition, the trustee has the power to delegate his or her power to other agents.¹⁰⁹

In the exercise of his or her powers, the trustee has specific obligations to the trust beneficiaries under the trust instrument, under state law, and under common law. Among the trustee duties in the Uniform Trust Code are the following: the duty to “administer the trust in good faith, in accordance with its terms and purposes and the interests of the beneficiaries”;¹¹⁰ the duty to “administer the trust solely in the interests of the beneficiaries”;¹¹¹ and the duty to “take reasonable steps to take control

98. *Id.* § 3-611(b).

99. UNIF. TRUST CODE § 103 cmt. (amended 2010).

100. *See, e.g., id.* §§ 815–16.

101. *Id.* § 401.

102. *Id.* § 701(a).

103. *Id.* § 702.

104. *Id.* § 815(a)(1).

105. *Id.* § 815(a)(2)(A).

106. *Id.* § 815(a)(2)(B).

107. *Id.* § 816(1).

108. *E.g., id.* § 816(2)–(3), (10)–(12), (19), (21)–(22), (26).

109. *Id.* § 807(a).

110. *Id.* § 801; *see also id.* § 105(b)(2).

111. *Id.* § 802(a).

of and protect the trust property.”¹¹² In addition, if the trustee has special skills or expertise, the trustee has a duty to use those special skills or expertise.¹¹³

Should the trustee fail to adequately meet his or her duties, there are remedies available to the persons interested in the trust. The trustee could be removed for committing a serious breach of trust or for a persistent failure to administer the trust effectively.¹¹⁴ A court also could “compel the trustee to perform the trustee’s duties”;¹¹⁵ reduce a trustee’s compensation;¹¹⁶ or “appoint a special fiduciary to take possession of the trust property and administer the trust.”¹¹⁷

B. *Presenting the Problems*

These four bodies of fiduciary law play an integral role in protecting and managing property regardless of its form. Despite this, digital property poses unique problems to the planning and execution stages of these fiduciary frameworks, particularly in the context of the Internet. This section discusses the complications that account holders, fiduciaries, and digital service providers face when dealing with fiduciary management of digital property. The table on the following page summarizes the problems posed to each body of fiduciary law:

112. *Id.* § 809.

113. *Id.* § 806.

114. *Id.* § 706(a)–(b).

115. *Id.* § 1001(b)(1).

116. *Id.* § 1001(b)(8).

117. *Id.* § 1001(b)(5).

Bodies of Fiduciary Law				
	Power of Attorney	Conservatorship	Probate Administration	Trust
Account Holders' Issues	Sharing account access information with fiduciaries may violate some TOSs.			
			Some service providers terminate accounts and account contents at death.	
				TOSs may prohibit transfer of title for accounts to the trustee.
Fiduciaries' Issues	With respect to the SCA, specific "lawful consent" for disclosure of account contents should come from the account holder.			
	A general grant of broad fiduciary authority under the governing instrument may not be sufficient.		A general grant of broad fiduciary authority under the governing instrument may not be sufficient.	
	General or specific authority under state fiduciary statutes may not be sufficient.			
	The fiduciary may not be able to give "lawful consent" on behalf of the account holder.			
	Accessing accounts may violate the TOS and computer crime laws on unauthorized access, creating the potential for criminal prosecution.			
	The fiduciary cannot compel service providers to disclose account content.			
				TOSs may prohibit transfer of title for accounts to fiduciaries.
Service Providers' Issues	Lawful consent may need to come from the account holder—fiduciary's consent may not be enough.			
	Voluntary disclosure of account contents may place service providers at risk of civil liability under the SCA.			
	Voluntary disclosure of account contents may constitute an unfair and deceptive trade practice, leading to charges by the federal FTC and state mini-FTCs.			
				Providers may be unaware of account holder's attempt to transfer title to the account to his or her trustee.

1. RESTRICTIONS ON ACCOUNT HOLDERS

In order to manage an account holder's digital property, a fiduciary must be able to access it. To facilitate access, the account holder may choose to disclose access information—such as usernames, account numbers, and passwords—or store that information where the fiduciary can access it. For some online accounts, this disclosure results in a violation of the TOS.¹¹⁸ For example, Facebook's TOS provides that “you will not share your password . . . , let anyone else access your account, or do anything else that might jeopardize the security of your account.”¹¹⁹ That TOS further provides that “[i]f you violate the letter or spirit of this Statement . . . , [Facebook] can stop providing all or part of Facebook to you.”¹²⁰ So, if an account holder were to provide his or her username and password to a fiduciary, then the account holder would violate Facebook's TOS and trigger Facebook's right to terminate the agreement—at which point the account holder might lose access to any digital property in the account. When service providers prohibit a fiduciary from learning an account holder's access information, they limit the account holder's ability to plan for the management of his or her digital property.

Another challenge is that the TOS for some accounts state that they terminate at an account holder's death. For instance, Yahoo!'s TOS provides 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 of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.”¹²¹ If an account and its contents will no longer exist after an account holder's death, how can the account holder properly plan to have it managed for and distributed to his or her beneficiaries? The seemingly clear answer: he or she cannot.

2. RESTRICTIONS ON THE FIDUCIARIES

When a fiduciary uses an account holder's username and password

118. In a survey conducted by the authors, thirteen of twenty popular service providers either prohibited account holders from disclosing their account access information or made account holders responsible to keep their access information private or secure. Memorandum from Peter J. Rademacher on Survey of Digital Serv. Provider Terms of Serv. to Christina L. Kunz (July 16, 2013) (on file with authors).

119. *Statement of Rights and Responsibilities*, FACEBOOK, <https://www.facebook.com/legal/terms> (last revised Dec. 11, 2012).

120. *Id.*

121. *Terms of Service*, YAHOO!, <http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html> (last updated Mar. 16, 2012).

to access and manage the account's digital property, that fiduciary may risk criminal liability under federal and state criminal statutes.

At the federal level, fiduciaries who exercise their powers over digital property without authorization risk potential criminal prosecution under the Computer Fraud and Abuse Act of 1984 ("CFAA").¹²² The CFAA provides criminal sanctions¹²³ against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."¹²⁴ A "protected computer" includes all computers "used in or affecting interstate or foreign commerce or communication."¹²⁵ In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, the United States District Court for the Western District of Washington determined that "since the advent of the Internet, almost all computer use has become interstate in nature[,] by their ability to access the Internet."¹²⁶ That makes sense, given the fact that the Internet is certainly an interstate communication forum. In *United States v. Mitra*, the United States Court of Appeals for the Seventh Circuit further clarified that any instrument used to access the Internet falls within the definition of "computer" under the CFAA.¹²⁷ Thus, an account holder's home computer, laptop, notepad, and smartphone may all qualify as protected "computers" under the CFAA, because they can all be used to access the Internet.¹²⁸ Furthermore, the CFAA's umbrella term may also cover computers and servers that support service providers.

While the CFAA does not define "authorization" or "authorized access," the United States Court of Appeals for the Ninth Circuit has interpreted the term to mean any permission at all.¹²⁹ Even under this broad definition, it is unclear how a court would rule on the question of whether a fiduciary, by his or her office, would have "authorization" to access the computers that house the accounts offered by service provid-

122. 18 U.S.C. § 1030 (2012).

123. *Id.* § 1030(c).

124. *Id.* § 1030(a)(2)(c).

125. *Id.* § 1030(e)(2).

126. 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000).

127. 405 F.3d 492, 495–96 (7th Cir. 2005) (concluding that the CFAA applies to any devices with capabilities comparable to a computer, including cell phones and iPods), *aff'd*, 134 F. App'x 963 (7th Cir. 2005), *cert. denied sub nom.* *Mitra v. United States*, 546 U.S. 979 (2005).

128. Greg Pollaro, iBrief, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, DUKE L. & TECH. REV., at ¶ 8 (2010) ("The inclusion of all computers used in interstate communication had a profound effect, intentionally or otherwise, as any computer connected to the Internet could be considered a 'protected computer' under the CFAA." (citation omitted)).

129. *See, e.g.*, *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132–33 (9th Cir. 2009) (applying the interpretive canons of plain meaning interpretation and rule of meaningful variation to define "authorization" as any permission at all).

ers, via the account of an account holder. If the account holder provided no formal documentation to show authorization, then a court would likely answer this question in the negative. But even if an account holder were to give a fiduciary formal authorization, the fiduciary may still be in danger of breaking the law. Because access to an account holder's account invariably requires accessing a service provider's or a third-party vendor's computers, the fiduciary must obtain not only the account holder's authorization, but also the service provider's authorization. As discussed earlier, service providers may prohibit third-party access to accounts.¹³⁰ For example, Facebook's TOS provides that "[y]ou will not solicit login information or *access an account belonging to someone else*."¹³¹ So, although the account holder may authorize the fiduciary to access the account, the fiduciary may be exceeding authorized access—within the meaning of the CFAA—by logging into the Facebook account if that access violates Facebook's TOS.

This perspective is consistent with statements made by agents of the United States Department of Justice ("DOJ"). The DOJ has asserted that the CFAA is broad enough to prosecute those who violate TOSs,¹³² as made clear by Richard Downing, Deputy Chief of the DOJ's Computer Crime and Intellectual Property Section, Criminal Division, in testimony before the House Subcommittee on Crime, Terrorism, and National Security.¹³³ However, Downing was careful to explain that the "DOJ is in no way interested in bringing cases against people who lie about their age on a dating site or anything of the sort. [The DOJ does not] have time or resources to do that."¹³⁴ While these remarks and other factors reasonably suggest that the DOJ is unlikely to prosecute individuals for minor TOS violations, nevertheless, the potential for prosecution and the chilling effect on fiduciaries remain a reality.¹³⁵

130. See *supra* notes 118–19 and accompanying text.

131. *Statement of Rights and Responsibilities*, *supra* note 119 (emphasis added).

132. Declan McCullagh, *DOJ: Lying on Match.com Needs to Be a Crime*, CNET (Nov. 14, 2011, 11:58 PM), http://news.cnet.com/8301-31921_3-57324779-281/doj-lying-on-match.com-needs-to-be-a-crime/ (quotation omitted); see also Lamm, *supra* note 20, at 12.

133. See *Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. On the Judiciary*, 112th Cong. 5, 14 (2011) (statement of Richard W. Downing, Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice) [hereinafter *Hearing*]; see also Lamm, *supra* note 20, at 12.

134. *Hearing*, *supra* note 133, at 69.

135. See Jim Lamm, *Planning Ahead for Access to Contents of a Decedent's Online Accounts*, DIGITAL PASSING (Feb. 9, 2012), <http://www.digitalpassing.com/2012/02/09/planning-ahead-access-contents-decedent-online-accounts/> (referencing state felony charges against defendant for accessing his wife's Gmail account); Kelsey T. Patterson, Note, *Narrowing It down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 519 & n.197 (2013) (citing *United States v. Nosal*, 676 F.3d 854, 860, 862 (9th Cir.

R

R

R

R

R

As if the CFAA were not enough to deter a fiduciary from executing his or her obligations, all fifty states criminalize unauthorized access to computers, systems, or networks (some requiring additional acts in conjunction with access itself).¹³⁶ Each statute is codified differently, but many share the following elements: (1) access to a computer, system, or network; (2) with knowledge; and (3) without authorization or in excess of authority.¹³⁷ As with the CFAA, the real question under this framework is what “authorization” means. Many state statutes fail to define this term,¹³⁸ and only some provide definitions for phrases like “in excess of authority.”¹³⁹ These definitions typically are consistent with the CFAA.¹⁴⁰ Thus, under a similar framework as that just discussed for the federal CFAA, a fiduciary also faces criminal prosecution at the state level. This increases the likelihood of enforcement and the potential penalty.

There is little indication how a court might rule regarding the potential conflict between state probate law and state criminal law, so this has a significant chilling effect—a fiduciary cannot execute his or her obligations regarding digital property without risking state criminal prosecution. On the other hand, a fiduciary has a duty under state law to manage an account holder’s designated property, including digital property. This crosscurrent of laws and duties leaves the fiduciary in an untenable position.

2012) (“The government assures us that, whatever the scope of the CFAA, it won’t prosecute minor violations. But we shouldn’t have to live at the mercy of our local prosecutor.”).

136. See, e.g., ALASKA STAT. § 11.46.740 (2013); IND. CODE § 35-43-2-3(b) (2013); MASS. GEN. LAWS ch. 266 § 120F (2013); MINN. STAT. § 609.891(1), (4) (2013); S.D. CODIFIED LAWS § 43-43B-1(1)–(2) (2013); VT. STAT. ANN. tit. 13, § 4102 (2013); see also *Computer Hacking and Unauthorized Access Laws*, NAT’L CONF. OF STATE LEGISLATURES, www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx (last updated June 19, 2012) (listing the relevant statutes for all fifty states). For a more expansive list of and explanation of state statutes criminalizing unauthorized access, see Memorandum from Peter J. Rademacher & Lucie O’Neill to the Drafting Committee on Fiduciary Access to Digital Assets on Issues Pertaining to Unauthorized Access Statutes (Aug. 8, 2012) (on file with authors and the Uniform Law Commission).

137. See, e.g., ARIZ. REV. STAT. ANN. § 13-2316(A)(8) (2013).

138. See, e.g., ALASKA STAT. § 11.46.740; ARIZ. REV. STAT. ANN. § 13-2316; MASS. GEN. LAWS ch. 266 § 120F.

139. E.g., COLO. REV. STAT. § 18-5.5-101(6.7) (2013).

140. Compare, e.g., *id.* (“‘Exceed authorized access’ means to access a computer with authorization and to use such access to obtain or alter information, data, computer program, or computer software that the person is not entitled to so obtain or alter.”) with 18 U.S.C. § 1030(e)(6) (2012) (“[T]he term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter[.]”).

3. RESTRICTIONS ON DIGITAL SERVICE PROVIDERS

Fiduciaries are not the only ones facing statutory conflicts. In 1986, Congress passed the Electronic Communications Privacy Act (“ECPA”).¹⁴¹ Title 2 of that Act, known as the Stored Communications Act (“SCA”),¹⁴² prohibits public providers of electronic communication services (“ECS”)¹⁴³ from “knowingly divulg[ing] to any person or entity the contents of a communication which is carried or maintained on that service”¹⁴⁴ In addition, it prohibits public providers of remote computing services (“RCS”)¹⁴⁵ from “knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service”¹⁴⁶ Finally, the SCA prohibits public providers of either ECSs or RCSs from “knowingly divulg[ing] a record or other information pertaining to a subscriber to or customer of such service”¹⁴⁷ Often, service providers provide ECSs and RCSs simultaneously, with respect to different services.¹⁴⁸ For instance, a message sent and awaiting review by the recipient could be held by the service provider as a provider of an ECS, while a photograph stored for private or public viewing could be held by the service provider as a provider of an RCS.¹⁴⁹ A practical example of this occurred in *Crispin v. Christian Audigier, Inc.*, where the United States District Court for the Central District of California held that Facebook acted as an ECS for purposes of private messaging, while it acted alternatively as an ECS or RCS for purposes of wall postings and comments.¹⁵⁰ Thus, all restrictions under

141. Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 1367, 2701–2711, 3117, 3121–3127 (2012)).

142. 18 U.S.C. §§ 2701–2711.

143. “[E]lectronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications” *Id.* § 2510(15). An “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facility or related electronic equipment for the electronic storage of such communications.” *Id.* § 2510(14). Providers of electronic communication services hold files in temporary electronic storage. See Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1215 n.48 (2004). “For example, ‘telephone companies and electronic mail companies’ generally act as providers of electronic communication services.” *Id.* at 1214 n.38 (citing S. REP. NO. 99-541, at 14 (1986), reprinted in 1986 U.S.C.A.N. at 3568).

144. § 2702(a)(1).

145. *Id.* § 2711(2) (“[T]he term ‘remote computing service’ means the provision to the public of computer storage or processing services by means of an electronic communications system”). Providers of remote computing services hold files primarily as a storage or processing service. See Kerr, *supra* note 143, at 1215 n.48.

146. § 2702(a)(2).

147. *Id.* § 2702(a)(3).

148. See Kerr, *supra* note 143, at 1215–16.

149. See *id.* at 1216 (providing a similar example).

150. See 717 F. Supp. 2d 965, 980–82, 989–90 (C.D. Cal. 2010).

R

R

the SCA may apply to any one service provider.

However, the SCA does not apply in all instances. It excludes *private* providers of ECSs and RCSs, such as a private e-mail service offered by an employer to employees or by a school to students.¹⁵¹ Furthermore, it does not prohibit an RCS provider from disclosing communications if the provider is authorized to access the content.¹⁵² Finally, it does not prohibit ECS or RCS providers from providing non-governmental entities with non-content records pertaining to account holders, such as the name of the person or entity attached to the account.¹⁵³

Even when the SCA does apply, there are exceptions. Among these is the right to disclose information “with the *lawful consent* of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of [RCSs].”¹⁵⁴ Notably, this exception *allows, but does not require* disclosure by a public provider of an ECS or RCS.¹⁵⁵

The primary issue with the SCA is much the same as that with the CFAA. Just as the CFAA does not define “authorization,” the SCA does not define “lawful consent.” In the context of the SCA, case law provides no clear answer regarding whether a fiduciary can provide “lawful consent” to a service provider. In *In re Facebook, Inc.*, the decedent’s mother wished to investigate the cause of the decedent’s death.¹⁵⁶ The mother, who was also the executor, was granted leave to subpoena records from the decedent’s Facebook account.¹⁵⁷ Facebook moved to quash the subpoena, which sought to compel Facebook to provide private information from the decedent’s account.¹⁵⁸ Facebook argued that it was unclear whether an executor, standing in the shoes of the decedent, could provide “lawful consent” for Facebook to divulge private information.¹⁵⁹ While the court suggested that the executor’s consent was suffi-

151. See § 2702(a)(1)–(2) (specifying that the prohibitions apply to a provider providing service to the *public*, as opposed to providing the service to a *private* entity).

152. See *id.* § 2702(a)(2)(B).

153. See *id.* § 2702(a)(3).

154. *Id.* § 2702(b)(3) (emphasis added).

155. See *id.* § 2702(b).

156. 923 F. Supp. 2d 1204, 1205 (N.D. Cal. 2012); see also Jeff John Roberts, *Dead Model’s Parents Can’t Get Facebook Messages, Judge Says*, GIGAOM (Sept. 27, 2012, 11:14 AM), <http://gigaom.com/2012/09/27/dead-models-parents-cant-get-facebook-messages-judge-says/>.

157. See *id.*

158. See *id.*

159. Facebook, Inc.’s Motion to Quash Subpoena in a Civil Case at 6–7, *In re Facebook, Inc.*, 923 F. Supp. 2d 1204 (N.D. Cal. 2012) (No. C 12-80171 LHK (PSG)), 2012 WL 8505651.

cient,¹⁶⁰ the court ultimately declined to rule on the issue.¹⁶¹ And even if the court had determined that the executor could give lawful consent on behalf of the decedent, the SCA does not *require* a service provider to disclose private account records, but merely authorizes *voluntary* disclosure.¹⁶² The court ultimately concluded that Facebook could not be compelled to turn over the account contents in a civil action.¹⁶³

The reality is that service providers have been reluctant to risk civil liability for disclosing private information. This is especially true given the growing number of account holders, the high cost of litigation, and the lack of profit to be gained from those disclosures. While the court's dictum in *In re Facebook, Inc.* suggests that fiduciaries can provide consent on behalf of account holders, it does not provide digital service providers with certainty that they can rely on when facing the possibility of civil liability. Thus, service providers have been understandably cautious about disclosing information when the SCA applies.

To deter wrongful disclosure, the SCA does not operate alone. The Federal Trade Commission ("FTC") prevents commercial entities "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."¹⁶⁴ To this end, the FTC can prevent service providers and other commercial entities from violating the PPs they use to draw consumers to their products and services.¹⁶⁵ The FTC's Web site expressly provides: "When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up [to] these promises."¹⁶⁶

Living up to its mission, the FTC has brought dozens of charges against various service providers, including Twitter,¹⁶⁷ Facebook,¹⁶⁸

160. *In re Facebook, Inc.*, 923 F. Supp. 2d at 1206 ("Of course, nothing prevents Facebook from concluding on its own that [the executor has] standing to consent on [the decedent's] behalf and providing the requested materials voluntarily.").

161. *See id.* ("[C]ase law confirms that civil subpoenas may not compel production of records from providers like Facebook.").

162. 18 U.S.C. § 2702(b)–(c) (2012) ("A provider . . . may divulge the contents of a communication [if an exception applies]." (emphasis added)).

163. *See In re Facebook, Inc.*, 923 F. Supp. 2d at 1206 ("Under the plain language of Section 2702, while consent may *permit* production by a provider, it may not *require* such a production." (emphasis in original) (citation omitted)).

164. 15 U.S.C. § 45(a)(2) (2012).

165. *Making Sure Companies Keep Their Privacy Promises to Consumers*, FED. TRADE COMM'N, <http://www.ftc.gov/opa/reporter/privacy/privacypromises.html> (last modified Sept. 4, 2013).

166. *Id.*

167. *See* Twitter, Inc., 151 F.T.C. 162 (2011).

168. *See* Facebook, Inc., No. 092-3184, 2011 WL 6092532 (Nov. 29, 2011).

MySpace,¹⁶⁹ and Google.¹⁷⁰ Thus, if a service provider chooses to violate its PP by disclosing private information to a fiduciary, it opens itself up to potential action by the FTC, as well as the public distrust that comes with public actions.

In addition to the federal FTC, states have their own “Little FTC Acts” that give states (and sometimes private parties) the power to bring similar claims for deceptive practices.¹⁷¹ States are typically given authority to seek “‘cease and desist order[s]’ or other injunctive relief, . . . declaratory judgment[s], or . . . settlement agreement[s].”¹⁷²

Under this federal and state framework, service providers face not only greater chances of being penalized but also severe penalties.¹⁷³ Thus, service providers remain reluctant to disclose private information to fiduciaries unless their PPs expressly permit such disclosure.

Finally, if civil sanctions under the SCA and charges brought by the federal and state FTCs were not enough to dissuade service providers from voluntarily disclosing private information, potential civil claims by concurrent or successor fiduciaries (on behalf of the account holder or beneficiaries) might be enough to dissuade service providers from disclosure.¹⁷⁴

IV. PURPORTED SOLUTIONS AND THEIR SHORTCOMINGS

Various private and public entities have proposed solutions to alleviate the problems that account holders, fiduciaries, and service providers face in the context of fiduciary management of digital property. This section discusses those proposed solutions and illustrates potential shortcomings.

A. *Private Entities Promoting Private or Commercial Planning Strategies*

Private legal and commercial entities have provided account holders with options for digital estate planning, social media wills or trusts, and digital legacy services, which attempt to move the estate planning

169. See Myspace LLC, No. 102-3058, 2012 WL 4101790 (Aug. 30, 2012).

170. See Google Inc., No. 102-3136, 2011 WL 5089551 (Oct. 13, 2011).

171. See Jack E. Karns, *State Regulation of Deceptive Trade Practices Under “Little FTC Acts”: Should Federal Standards Control?*, 94 DICK. L. REV. 373, 375 & n.10 (1990).

172. CHRISTINA L. KUNZ & CAROL L. CHOMSKY, *CONTRACTS: A CONTEMPORARY APPROACH* 561 (2d ed. 2013).

173. Karns, *supra* note 171, at 374 (“Little FTC Acts have attractive remedy provisions that may permit treble damages.” (citation omitted)).

174. See UNIF. TRUST CODE §§ 706(a), 1001 cmt. (2010); UNIF. PROBATE CODE § 3-703(c) (amended 2010); UNIF. POWER OF ATTORNEY ACT § 116(a)(2) (2006); UNIF. GUARDIANSHIP AND PROTECTIVE PROCEEDINGS ACT §§ 112(b), 416(a)(3) (1998).

process into a digital medium. This section discusses how these options may fail to resolve all of the conflicts that account holders and fiduciaries face.

When probate attorneys, legal academics, and entrepreneurs realized the magnitude of digital property housed on computers and the Internet, they attempted to develop processes that would alleviate individuals' difficulties in estate planning for their digital assets. Referred to as "digital estate planning,"¹⁷⁵ this process involves step-by-step instructions for individuals or their attorneys to plan for the management of digital property, through so-called "social media wills."¹⁷⁶

Under a typical digital estate planning method, an individual should first—or at least early on—inventory his or her digital property, including online accounts where property is housed, as well as other digital property saved to the individual's hardware.¹⁷⁷ Second, the individual should record all account numbers or usernames with their respective passwords and preserve that account information digitally or in hardcopy.¹⁷⁸ Third, the individual should select a "digital fiduciary," who is not necessarily the same person who would perform other fiduciary functions.¹⁷⁹ A digital fiduciary often has technical qualifications that make him or her more capable of satisfying the account holder's desires regarding digital property.¹⁸⁰ Fourth, the individual should provide instructions regarding management of his or her digital property.¹⁸¹ These instructions help the digital fiduciary access accounts, communicate with service providers, manage digital property, and coordinate with other fiduciaries and interested persons. Finally, the individual should give the digital fiduciary the proper authorization.¹⁸² This entire process often takes the form of a "social media will" or trust—it can also be extended to conservatorships and powers of attorney—which purportedly isolates digital property from other more traditional prop-

175. See, e.g., Anderson, *supra* 19, at 44; Steven Maimes, *Managing Your Digital Afterlife: Cyber Footprint, Ownership, and Access*, THE TRUST ADVISOR (Jan. 28, 2013), <http://thetrustadvisor.com/headlines/digital-afterlife>. R

176. See, e.g., Gen. Servs. Admin., *Write a Social Media Will*, <http://www.usa.gov/topics/money/personal-finance/wills.shtml> (last updated Sept. 6, 2013); *Social Media Will*, ROCKET LAWYER, <http://www.rocketlawyer.com/document/social-media-will.rl> (last visited Oct. 19, 2013).

177. See Anderson, *supra* note 19, at 44 (listing inventorying of digital property as the second step); Frank S. Baldino, *Estate Planning and Administration for Digital Assets*, MD. B.J., Nov.–Dec. 2012, at 28, 30. R

178. See Baldino, *supra* note 177, at 30. R

179. See Anderson, *supra* note 19, at 45 (listing selection of a digital fiduciary as the fourth step). R

180. See *id.*

181. See *id.* (listing the provision of instructions as the fifth step).

182. See *id.*

erty.¹⁸³ Interestingly, the General Services Administration has encouraged this type of planning for digital property management.¹⁸⁴

Despite its immediate appeal, digital estate planning raises one primary issue. It may cause account holders to violate TOSs that prohibit them from disclosing their account access information to third parties, that prohibit transfer of the account itself, or that prohibit third parties from accessing their accounts. Any of these types of violations may trigger remedial rights specified in the TOSs, sometimes including termination of service.¹⁸⁵ Thus, digital estate planning nonetheless may be impeded by the contract issues that TOSs raise during the planning and execution processes.

Digital legacy services offer various combinations of these four categories of service:

- storing information such as account holders' passwords like a digital safe;¹⁸⁶
- recording and facilitating how the individual's digital estate plan will be implemented;¹⁸⁷
- performing specified tasks for the account holder, such as removing information from the list of accounts and passwords stored with the service, so that fiduciaries are not made aware of them;¹⁸⁸ or
- streamlining the management process through partnerships with service providers, and executing certain account-maintenance actions.¹⁸⁹

These services raise additional issues.

The first category of service does not work in the same manner as a social media will or trust. Instead, account holders are merely provided digital storage space for their account information. Still, if a digital legacy service permitted sharing, and if an account holder gave a fiduciary access to the digital legacy service account, the account holder may violate a service provider's TOS that prohibits sharing or disclosure of

183. See Gen. Servs. Admin., *supra* note 176.

184. See *id.*

185. E.g., *Myspace Services Terms of Use Agreement*, MYSPACE, <https://myspace.com/pages/terms> (last revised June 10, 2013) ("Myspace expressly reserves the right to remove your Profile or Content, in whole or in part, and/or deny, restrict, suspend, or terminate your access to all or any part of the Myspace Services, if Myspace determines, in its sole discretion, that you have violated this Agreement . . .").

186. *KeePass Password Safe*, KEEPASS, <http://keepass.info/> (last visited Sept. 4, 2013).

187. LEGACY LOCKER, <http://legacylocker.com/> (last visited Sept. 4, 2013).

188. CIRBUS LEGACY, <http://www.cirbuslegacy.com/> (last visited Sept. 4, 2013).

189. This is merely a hypothetical type of service that could be offered by digital legacy services. To our knowledge, none do.

access information.¹⁹⁰ In addition, the account holder may violate the digital legacy service's TOS if that TOS prohibits violating third-party service providers' TOSs.¹⁹¹ Finally, if the fiduciary were able to access the digital legacy service, the fiduciary might still be "exceeding authorized access" in violation of the TOS—risking criminal prosecution under the CFAA and state criminal laws by using the information he or she obtained on that digital legacy service to access the service providers.¹⁹²

The second and third categories of services are more consistent with the concepts of social media wills or trusts. These services are designed for account information and instructions to be transferred to fiduciaries when triggered.¹⁹³ These digital legacy services operate as a beneficiary designation with the purpose of transferring an account holder's account information when triggered (typically at death). However, the benefit to the fiduciary sometimes comes with a proviso. Some digital legacy services provide that their services cannot be used in a manner that violates the TOS of a service provider.¹⁹⁴ Because many service providers prohibit disclosing account access information,¹⁹⁵ it is easy to violate this term by uploading or retrieving the account-access information. In addition, even if an account holder selects a digital legacy service that does not have a stated policy regarding violation of other TOSs, the digital fiduciary still risks potential criminal prosecution under the CFAA and state criminal laws.¹⁹⁶

In theory, there remains a fourth category of service offered by digital legacy services. These digital legacy services could establish partnerships with service providers that allow the digital legacy services to execute an account holder's wishes without the need to worry about authorization and TOS violations.¹⁹⁷ In other words, this type of service

190. Facebook's TOS provides: "You will not share your password . . . or do anything else that might jeopardize the security of your account." *Statements of Rights and Responsibilities*, *supra* note 119 (emphasis added). Myspace's TOS provides: "You agree not to . . . disclose your password to any third party." *MYSFACE*, *supra* note 185.

191. For example, SecureSafe's TOS provides: "The customer is obligated to ensure that he can provide data access to the Beneficiaries *without violating third party rights* or applicable statutory provisions." *Standard Terms and Conditions of Business (T&C)*, *SECURESAFE* (Nov. 21, 2012), <http://www.securesafe.com/en/terms.html> (emphasis added).

192. *See supra* Part III.B.2.

193. The trigger is typically confirmation of death because these services are intended as a medium for instructing posthumous wishes. *See CIRRUS LEGACY*, *supra* note 188 ("What happens to my online life when I die?"); *LEGACY LOCKER*, *supra* note 187 ("Legacy Locker is a safe, secure repository for your vital digital property that lets you grant access to online assets for friends and loved ones in the event of loss, death, or disability.").

194. *See SECURESAFE*, *supra* note 191.

195. *See Statements of Rights and Responsibilities*, *supra* note 119.

196. *See supra* Part III.B.2.

197. At one time, such a digital legacy service did exist. *See Your Digital Assets After Death*,

would not only operate as a social media will or trust; it could also operate as a digital beneficiary designation for the account itself and the account's content (not just transferring account access information). This category of service would present unique issues.¹⁹⁸

Regardless of the unique legal issues that each type of service raises, digital legacy services present practical issues for account holders. Digital legacy services are often developed as small start-up companies or concepts by systems architects, engineers, or programmers.¹⁹⁹ Sometimes, these founders might not realize the potential demand of their digital legacy services until they have grown beyond their original conceptions. Other times, these founders may lose money in their digital legacy services. Because of these unknowns, digital legacy services can be sold, can go out of business, or can go into bankruptcy.²⁰⁰ If the sale or shut down were to wipe out an account holder's digital legacy services account, he or she could lose data and even his or her entire digital estate plan. Moreover, an account holder might not find out about the digital legacy service's demise before becoming incapacitated or dying.

In addition to their potential unreliability, digital legacy services—particularly those offering the second, third, and fourth categories of services—purport to facilitate complete and valid estate planning for digital property, when in fact they may not,²⁰¹ and these services may conflict with the individual's estate plan expressed in a will or revocable trust. Thus, account holders could spend time and money to receive a service that they may not, in fact, ultimately receive. In the extreme, this con-

ROCKETBOOM (Apr. 2, 2010), <http://www.rocketboom.com/digital-assets/>. However, it appears that Entrustet, and subsequently SecureSafe, acquired this program; the services offered are now unclear. See *Welcome Entrustet Users!*, SECURESAFE, <http://www.securesafe.com/en/partners/entrustet.html> (last visited Oct. 19, 2013); Gerry W. Beyer & Naomi Cahn, *Digital Planning: The Future of Elder Law*, 9 NAELA J. 135, 152 n.81 (2012).

198. Under such a scenario, three contracts would exist: (1) between the account holder and the service provider, (2) between the account holder and the digital legacy service, and (3) between the service provider and the digital legacy service. The first and third contracts would likely conflict on the terms regarding the account holder's disclosure of his or her access information and the service provider's disclosure of the account holder's private information. There are canons of contract construction that could resolve these issues. For example, later contracts prevail over prior contracts and more specific terms prevail over more general terms. However, courts may not always apply these canons properly, and the litigation costs to reach even a correct judicial conclusion could be great.

199. See Rob Walker, *Things to Do in Cyberspace when You're Dead*, N.Y. TIMES MAG., Jan. 9, 2011, at 30, available at http://www.nytimes.com/2011/01/09/magazine/09Immortality-t.html?pagewanted=all&_r=0.

200. Baldino, *supra* note 177, at 30; Beyer & Cahn, *supra* note 197, at 152 (“[Digital legacy services] come and go; their life is dependent upon the whims and attention spans of their creators and creditors.” (citation omitted)); see also Walker, *supra* note 199; *supra* note 197.

201. See Beyer & Cahn, *supra* note 197, at 152 (“Some of these companies purport to distribute digital assets to beneficiaries. . . . [T]hese companies cannot do this legally”).

duct could even arise to the level of an unfair and deceptive trade practice.

B. State Protection of Fiduciaries in Digital Property Management

Six states have enacted statutes explicitly granting personal representatives (and, in one case, conservators) power to access some types of digital property.²⁰² At least seventeen other states have proposed similar legislation.²⁰³ However, the inconsistencies among the existing state statutes pose yet another problem for fiduciaries trying to manage digital property. First, the statutes vary in the types of fiduciaries that are provided authority.²⁰⁴ Second, the statutes differ in scope. For instance, some statutes compel service providers to provide fiduciaries access to or copies of digital property,²⁰⁵ while others provide fiduciaries with authorization to access digital property;²⁰⁶ still others provide the fiduciaries with complete power to manage digital property.²⁰⁷ Third, the statutes differ on what types of accounts are covered. Connecticut and Rhode Island limit their statutes to e-mail services,²⁰⁸ others include social media and microblogging Web sites, and Indiana's is broad enough to include any information stored electronically by a custodian.²⁰⁹ If six states cannot create consistency in this area of law, fifty

202. CONN. GEN. STAT. § 45a-334a (2013); IDAHO CODE ANN. § 15-5-424(3)(z) (2011); IND. CODE § 29-1-13-1.1 (2013); OKLA. STAT. tit. 58, § 269 (2013); R.I. GEN. LAWS § 33-27-2 (2011); VA. CODE ANN. § 64.2-110 (2012).

203. See, e.g., S. 279, Reg. Sess. (N.C. 2013), available at <http://www.ncleg.net/Sessions/2013/Bills/Senate/PDF/S279v1.pdf>; S. 54, 77th Legis. Assemb., Reg. Sess. (Or. 2013), available at <https://olis.leg.state.or.us/liz/2013R1/Measures/Text/SB54/Introduced>; S. 2313, 187th Leg., Reg. Sess. (Mass. 2012), available at <https://malegislature.gov/Bills/187/Senate/S02313>; Leg. 783, 102d Leg., 2d Sess. (Neb. 2012), available at <http://www.nebraskalegislature.gov/FloorDocs/102/PDF/Intro/LB783.pdf>; Assemb. 9317, 2011-12 Gen. Assemb., Reg. Sess. (NY 2012), available at http://assembly.state.ny.us/leg/?default_fld=&bn=A09317&term=2011&Text=Y; H.R. 2580, Reg. Sess. (Pa. 2012), available at <http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2011&sessInd=0&billBody=H&billTyp=B&billNbr=2580&pn=3959>; Jim Lamm, *August 2013 List of State Laws and Proposals Regarding Fiduciary Access to Digital Property During Incapacity or After Death*, DIGITAL PASSING (Aug. 30, 2013), <http://www.digitalpassing.com/2013/08/30/august-2013-list-state-laws-proposals-fiduciary-access-digital-property-incapacity-death/>.

204. Compare IDAHO CODE ANN. § 15-5-424 (providing conservators authority) with OKLA. STAT. tit. 58, § 269 (providing personal representatives authority).

205. E.g., CONN. GEN. STAT. § 45a-334a ("An [ECS] provider shall provide, to the executor or administrator of the estate of a deceased person . . . access to or copies of the contents of the [ECS]" (emphasis added)).

206. OKLA. STAT. tit. 58, § 269 ("The executor or administrator of an estate shall have the power . . . 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." (emphasis added)).

207. IDAHO CODE ANN. § 15-5-424(3)(z); see also Baldino, *supra* note 177, at 30.

208. CONN. GEN. STAT. § 45a-334a; R.I. GEN. LAWS § 33-27-3 (2011).

209. IND. CODE § 29-1-13-1.1 (2013).

states may exacerbate the convolution for laypersons and service providers.

In addition to the confusion that the statutes create themselves, fiduciaries must also consider which state statute applies for each service provider, given the fact that many service providers include choice-of-law clauses in their TOSs.²¹⁰ For instance, it is possible that Oklahoma's statute may not apply to a service provider with a California choice-of-law clause in its TOS, even if the account holder and fiduciary reside in Oklahoma. Courts usually enforce choice-of-law clauses if they bear a reasonable relation (not necessarily the most significant relation) to the transaction.²¹¹ Although a court might void a choice-of-law clause—as a matter of public policy—if the chosen state law ran too contrary to the applicable fiduciary law of the court's state,²¹² public policy is rarely recognized as a defense. Thus, the digital property in a particular estate might well be governed by many state statutes or the laws of another country, as invoked by the various TOSs that govern various accounts of the incapacitated or deceased person.

V. A HOLISTIC APPROACH TO RESOLUTION

The CFAA, the SCA, state criminal laws, privacy laws, and TOSs all present obstacles to account holders attempting to plan for their digital estates, fiduciaries attempting to manage digital property, and service providers attempting to remain out of the courts. Resolving a multifaceted problem requires a multifaceted approach. This section provides alternative solutions tailored to the individual problems faced by account holders, fiduciaries, and service providers. Note that the proposed solutions are legislative because the court system cannot resolve the statutory issues discussed in this Article and will be hard-pressed to keep up with the evolving technological issues. Thus, a clear and comprehensive solution at common law is unrealistic.

210. Google provides that “[t]he laws of California, U.S.A., excluding California’s conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services.” *Google Terms of Service*, GOOGLE, <http://www.google.com/intl/en/policies/terms/> (last updated Mar. 1, 2012). Activision Blizzard provides that the agreement between it and World of Warcraft account holders “shall be governed by, and will be construed under, the laws of the United States of America and the law of the State of Delaware, without regard to choice of law principles.” *World of Warcraft Terms of Use*, *supra* note 21. These are two of many similarly drawn provisions.

211. *See, e.g.*, *Cantu v. Jackson Nat’l Life Ins. Co.*, 579 F.3d 434, 437–438 (5th Cir. 2009); *United Cntys. Trust Co. v. Mac Lum, Inc.*, 643 F.2d 1140, 1143 (5th Cir. 1981); *Burroughs Corp. v. Suntogs of Miami, Inc.*, 472 So. 2d 1166, 1167 (Fla. 1985); *Aerospatiale Helicopter Corp. v. Universal Health Servs., Inc.*, 778 S.W.2d 492, 499 (Tex. App. 1989).

212. *Cf.* Case Note, *Fundamental Public Policy—Per Se Rule or Case-by-Case Determination: Modern Computer Systems v. Modern Banking Systems*, 23 CREIGHTON L. REV. 601, 618–20 (1990) (discussing court opinions upholding state franchise laws over choice-of-law provisions).

The section concludes with a set of best practices that can reduce the risks borne by account holders and fiduciaries in the interim. Although these practices do not eliminate risk for account holders and fiduciaries, they limit the risk, which is the only option account holders and fiduciaries have, besides doing nothing with digital property at all.

A. *Congressional Amendments*

The first solution to the issue discussed in this article could come from Congress, in the form of amendments to the SCA and CFAA. These amendments would both resolve uncertainty regarding the application of those statutes and provide persuasive arguments for preventing the application of state criminal laws.

The SCA could be amended by augmenting § 2711 to define “lawful consent,” thereby eliminating any question about whether or not lawful consent is satisfied through state laws governing fiduciary fields. The new SCA definition could read as follows:

(5) the term “lawful consent” means cognizable permission, either tangible or digital, that has lawfully been executed by or on behalf of any party whose consent is required, including, but not limited to, by any fiduciary representing the party under state law, and remains in force. Lawful consent can be given either expressly or implicitly pursuant to federal or state law or court order.

Likewise, the CFAA could be amended by augmenting § 1030(e) to define “authorization,” eliminating any question about whether authorization is satisfied by fiduciary appointments governed under state law. This new definition would appear at § 1030(e)(6), and all other definitions within § 1030(e) would shift to accommodate it. It could read as follows:

(6) the term “authorization” means cognizable permission, either tangible or digital, that has lawfully been executed by or on behalf of any party whose authorization is required, including, but not limited to, by any fiduciary representing the party under state law, and remains in force. Authorization can be given either expressly or implicitly pursuant to federal or state law or court order. Authorization granted to one party shall extend to: (1) any fiduciary representing that party under state law, to the extent that the fiduciary’s appointment includes that authorization; and (2) a third party granted permission by either the original party or by any fiduciary representing the original party under state law. A fiduciary representing a party under state law may only grant authorization to a third party within the scope of that fiduciary’s authorization.

These amendments would also alleviate concerns that fiduciaries face regarding state criminal laws. Although state statutes can provide

their own definitions for “consent” or “authorization,” many of them have not.²¹³ If state courts were confronted with violations of unauthorized access statutes and had no definitions to interpret them, the definitions in the SCA and CFAA could be used as persuasive tools to interpret those statutes. Therefore, although the amendments only would directly affect the SCA and CFAA, they may serve to provide greater protections against state criminal statutes as well.

B. *Uniform State Law*

A uniform state law governing fiduciary management of digital property could create a consistent state framework to resolve conflicts with state criminal laws, as well as supplementing federal criminal and civil laws. Today, the Uniform Law Commission is exploring this very idea.²¹⁴ As of the date of this article, a discussion draft of the Fiduciary Access to Digital Assets Act (“FADA Act”) is published and under review by the Uniform Law Commission.²¹⁵ The FADA Act serves as a freestanding act or amendment that extends the provisions of certain other acts to the context of digital property. This article will address only the most relevant of the FADA Act’s provisions—sections 3 through 10.²¹⁶

Section 3 provides that all fiduciaries with authority over digital property have “the same authority as the account holder[s]” and have “the lawful consent of the account holder[s] and [are] . . . authorized user[s] of the account[s].”²¹⁷ Sections 4 through 7 then give agents, conservators, personal representatives, and trustees authority over digital property in their respective capacities.²¹⁸ However, each fiduciary is treated differently regarding how they receive authority. Under section 4, for example, the default rule is that a personal representative has authority over a decedent’s digital property,²¹⁹ while, under sections 5

213. See, e.g., ALASKA STAT. § 11.46.740 (2013); WIS. STAT. § 943.70 (2013); NEB. REV. STAT. §§ 28-1343, 28-1347 (2012).

214. *Committees: Fiduciary Access to Digital Assets*, UNIF. LAW COMM’N, <http://www.uniformlaws.org/Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets> (last visited Sept. 4, 2013).

215. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (Draft 2013), available at http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013AM_FADA_Draft.pdf.

216. For a more complete dissection of the FADA Act, see Samantha D. Haworth, *Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act*, 68 U. MIAMI L. REV. 535 (2014).

217. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 3 (Draft 2013), available at http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013AM_FADA_Draft.pdf.

218. *Id.* § 4 (personal representatives); *id.* § 5 (conservators); *id.* § 6 (agents); *id.* § 7 (trustees).

219. *Id.* § 4.

and 6, a conservator or agent must be given specific authority over a protected person's or principal's digital property.²²⁰ Finally, under section 7, a trustee is given authority over digital property held in the trust in accordance with the terms of the trust.²²¹

After sections 3 through 7 provide fiduciaries with authority and consent, section 8 provides the requirements for how each fiduciary may request to access, take ownership of, or copy digital property.²²² In addition, section 8 provides that "custodians" of digital property, or service providers, must comply with proper requests for access to, ownership of, or copying of digital property²²³ within a specified time period.²²⁴ And because section 8 has the potential to put service providers at risk of civil liability, the FADA Act also provides immunity for them.²²⁵

Finally, section 10 calls for courts to construe the FADA Act with consideration for "the need to promote uniformity of the law with respect to its subject matter among states that enact it."²²⁶

The FADA Act, though still in the drafting stage of its development, provides several key benefits. It is well-established in the common law that the personal representative of a deceased person's estate "stands in the shoes of the decedent" in administering that estate, and other fiduciaries have the authority to take actions necessary or incidental to achieve a principal's objectives, unless the principal directs otherwise.²²⁷ The FADA Act does not overturn these well-established fiduciary concepts. Instead, it clarifies that modern digital assets and accounts are within the scope of well-established fiduciary powers and authority. In addition, the FADA Act is intended to bridge the gap between state fiduciary laws and federal criminal and data privacy laws, particularly the issues of "authorization" under the CFAA and "lawful consent" under the SCA.²²⁸ To be sure, this raises questions of federalism and preemption. However, federal courts may look to state law to define terms for which federal statutes lack definition.²²⁹ If a significant number of states

220. *Id.* § 5 (conservators); *id.* § 6 (agents).

221. *Id.* § 7.

222. *Id.* § 8(c).

223. *Id.* § 8(b).

224. *Id.* § 8(d).

225. *Id.* § 9.

226. *Id.* § 10.

227. 31 AM. JUR. 2D *Executors and Administrators* § 372 (2013); see RESTATEMENT (THIRD) OF AGENCY § 2.02 (2006).

228. FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 3 cmt. (Draft 2013), available at http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013AM_FADA_Draft.pdf.

229. See, e.g., *De Sylva v. Ballentine*, 351 U.S. 570, 580 (1956) ("The scope of a federal right is, of course, a federal question, but that does not mean that its content is not to be determined by state, rather than federal law.").

enact the final FADA Act, then federal courts may be more inclined to look to the FADA Act to define “authorization” under the CFAA²³⁰ and “lawful consent” under the SCA.²³¹

In addition, if the states uniformly adopted the FADA Act, the issues surrounding TOSs’ choice-of-law clauses would be resolved. No longer could service providers insulate themselves by selecting the laws of states that do not compel disclosure of private information through statute.

C. *Best Practices in the Interim*

While practitioners, scholars, and legislators work on permanent solutions to the problems with fiduciary management of digital property, account holders and fiduciaries still have to plan for and manage digital property. To that end, they should take certain actions to increase their level of certainty and reduce their level of risk. These practices will reduce the likelihood that problems will arise before and during fiduciary management of digital property.

1. HOW ACCOUNT HOLDERS SHOULD PLAN FOR DEATH OR INCAPACITY

To increase certainty, account holders should take four steps to plan ahead. First, they should inventory their digital footprint by listing all accounts and whether the accounts or their contents have financial or sentimental value.²³² As part of this process, account holders should create a list of usernames, account numbers, and passwords.²³³ Due to this information’s sensitivity, account holders should take extra precautions to ensure that it does not end up in the wrong hands—including either encrypting an electronic list or securely storing a written list with instruction that the only person permitted access is a fiduciary.²³⁴

Second, to the extent possible, account holders should regularly back up any electronically stored information, especially when the information is stored remotely by service providers subject to the SCA.²³⁵ This way, fiduciaries would only deal with service providers for the purpose of closing or memorializing accounts, while accessing locally stored data and backups for collecting, managing, and distributing digital property. If fiduciaries avoid the need to access information that is

230. 18 U.S.C. § 1030(a)(2) (2012).

231. *Id.* § 2702(b)(3).

232. *See* LAMM, *supra* note 20, at 6.

233. *Id.*

234. *Id.* at 7–8, 10–11.

235. *Id.* at 10.

stored remotely by service providers, then the fiduciaries also avoid the potential problems of federal and state data privacy laws and computer crime laws related to accessing remotely-stored information.

Third, account holders should make a plan for managing and distributing the digital property they have inventoried.²³⁶ This plan should include designating a fiduciary under a power of attorney, trust, or will with clear powers and authority over digital property.²³⁷ The plan should also include instructions for distributing the content to beneficiaries, abandoning or eliminating any digital property that is worthless, and securely deleting any specified digital property the individual does not want to pass on.²³⁸

Fourth, account holders should expressly authorize service providers to disclose their private information to their fiduciaries.²³⁹ This authorization should clearly state the account holder's intention to satisfy the CFAA, SCA, state criminal laws, and privacy laws, to ensure that the fiduciaries and service providers have evidence of the individual's "lawful consent" and "authorized access."²⁴⁰ The following is a sample will provision:

Powers and authorizations regarding digital property. The personal representative may exercise all powers that an absolute owner would have and any other powers appropriate to achieve the proper investment, management, and distribution of: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; (4) any user account of mine; and (5) any domain name of mine. The personal representative may obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that information. I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to the personal representative: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended; and any other applicable federal or state data privacy law

236. *Id.* at 11–12.

237. *Id.* at 11–13.

238. *See id.* at 11.

239. *Id.* at 9.

240. *Id.* at 11–12.

or criminal law. The personal representative may employ any consultants or agents to advise or assist the personal representative in decrypting any encrypted electronically stored information of mine or in bypassing, resetting, or recovering any password or other kind of authentication or authorization, and I hereby authorize the personal representative to take any of these actions to access: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; and (4) any user account of mine. The terms used in this paragraph are to be construed as broadly as possible, and the term “user account” includes without limitation an established relationship between a user and a computing device or between a user and a provider of Internet or other network access, electronic communication services, or remote computing services, whether public or private.²⁴¹

Note that this provision addresses disclosure, as well as authorized access. Also note that the provision could be manipulated to authorize an agent under a power of attorney or a trustee under a trust.

The following is a stand-alone authorization and consent document that could be executed separately from a power of attorney, will, or trust document:

Authorization and Consent for Release of Electronically Stored Information

I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to my then-acting fiduciaries at any time: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. The terms used in this authorization are to be construed as broadly as possible, and the term “fiduciaries” includes an attorney-in-fact acting under a power of attorney document signed by me, a guardian or conservator appointed for me, a trustee of my revocable trust, and a personal representative (executor) of my estate.

This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended; and any other applicable federal or state data privacy law or criminal law. This authorization is effective immediately. Unless this authorization is revoked by me in writing while I am competent, this authorization

241. *See id.* at 12–13.

continues to be effective during any period that I am incapacitated and continues to be effective after my death.

Unless a person or entity has received actual notice that this authorization has been validly revoked by me, that person or entity receiving this authorization may act in reliance on the presumption that it is valid and unrevoked, and that person or entity is released and held harmless by me, my heirs, legal representatives, successors, and assigns from any loss suffered or liability incurred for acting according to this authorization. A person or entity may accept a copy or facsimile of this original authorization as though it were an original document.²⁴²

This sample addresses all the fiduciary types that this article has addressed. However, note that the sample provision only addresses consent to *disclose* information, not authorization to *access*, which would be handled separately in a power of attorney, will, or trust document or in a court order appointing a conservator or a personal representative.

2. HOW FIDUCIARIES SHOULD MANAGE PROPERTY WHEN NO PLAN EXISTS

To reduce risk, in the event the decedent or incapacitated failed to plan ahead, fiduciaries should take five steps. First, any fiduciary designated to access, manage, or distribute an individual's property, including digital property, should consult an attorney to evaluate the risk. This area of law is still developing and, to some extent, is unpredictable. Fiduciaries are well advised to gather as much information as they can, including the options they have at any given juncture in the process, before further engaging in digital-property management.

Second, fiduciaries should contact the service providers to request a copy of the contents of the decedent's or incapacitated person's valuable or significant accounts.²⁴³ Requesting a copy of the contents avoids the potential problems of attempting to directly access the account itself, which could constitute "unauthorized access" within the scope of the CFAA or state criminal laws.

Third, if there are any pending civil or criminal investigations involving the decedent, fiduciaries should not access or tamper with any digital property, so as to maintain complete and accurate copies of all data.²⁴⁴ In the event that accessing digital property is necessary, fiduciaries should consult with an attorney and a computer forensics expert to prevent altering or inadvertently deleting any digital property before or

242. *See id.* at 13.

243. *See id.* at 16.

244. *Id.* at 14–15.

during pending investigations.²⁴⁵

Fourth, if no investigation is pending, fiduciaries should still create exact image copies of all digital property before any other attempts to access the storage device or data, to the extent possible.²⁴⁶ This will ensure that information necessary for a computer forensics expert to retrieve or recover the digital property, including Web-browsing history and recently deleted files, are preserved.²⁴⁷ “Simply turning on and booting up a smartphone or computer can overwrite or wipe out data that may be useful in a [computer] forensic examination.”²⁴⁸

Fifth, in the event that fiduciaries lack information regarding what accounts a decedent or incapacitated person had, the content within those accounts, and the necessary access information, fiduciaries should consult with computer forensics experts to attempt to discover this information.²⁴⁹

VI. CONCLUSION

Account holders, fiduciaries, and service providers face tremendous obstacles regarding fiduciary management of digital property. Given the growing ownership, value, and significance of digital property, the exigency to resolve these problems is great. Despite this, legislatures, courts, and service providers have failed to fully address these problems. Furthermore, efforts at the private and public level so far have not provided clear and complete solutions to the risks that account holders, fiduciaries, and service providers face.

The different types of fiduciaries discussed in this article each face numerous problems raised by digital property. To resolve all of these problems, legislatures must take a multifaceted approach. At the federal level, the article provided simple amendments that would resolve the obstacles raised by the CFAA and the SCA. At the state level, legislatures can clarify the scope of fiduciary powers and authority in a uniform manner, influencing the impact of not only state laws, but also federal laws. Until the federal and state legislatures take these or similar steps, account holders, fiduciaries, and service providers can work to minimize their respective uncertainty and risk by providing clear fiduciary powers, authority, and instructions regarding digital property in powers of attorney, wills, trusts, and stand-alone documents to support existing or future fiduciary appointments.

245. *Id.*

246. *Id.* at 16.

247. *Id.* at 15.

248. *Id.*

249. *See id.*