Vanderbilt Law Review

Volume 67
Issue 6 *Issue 6 - November 2014*

Article 8

11-2014

The Stored Communications Act and Digital Assets

David Horton

The Stored Communications Act and Digital Assets

*David Horton**

Commentary on Naomi Cahn, *Probate Meets the Digital Age*[1]

I. INTRODUCTION

The story has become all too familiar. Someone dies, and her loved ones request the contents of her text, email, or social media accounts. Perhaps they wish to preserve this vibrant electronic slice of the decedent's life.[2] Perhaps grief compels them to sift through the minutiae of the decedent's final days.[3] Or perhaps they are merely trying to fulfill their duties as trustees, executors, or administrators to pay the decedent's bills and to inventory her property. However, the decedent's Internet Service Provider ("ISP")—be it Facebook, Yahoo!, or Microsoft—refuses to cooperate.

---

* Professor of Law, University of California, Davis, School of Law (King Hall).

Thanks to Naomi Cahn for helpful comments.

1. Naomi Cahn, Probate Law Meets the Digital Age: Harmonizing Federal Law With State Wealth Transfer Law on Digital Assets, 67 VAND. L. REV. 1697 (2014).

2. *See, e.g.*, Paresh Dave, *Grieving Dad Gets 'Look Back' Video for Dead Son From Facebook*, L.A. TIMES (Feb. 7, 2014), http://articles.latimes.com/2014/feb/07/nation/la-na-nn-facebook-dead-son-20140207, *archived at* http://perma.cc/FUD3-8NBK (recounting a father's struggle to obtain a copy of a video of his deceased son from Facebook).

3. *See, e.g.*, Geoffrey A. Fowler, *Life and Death Online: Who Controls a Digital Legacy*, WALL ST. J. (Jan. 5, 2013), http://online.wsj.com/news/articles/SB10001424127887324677204578188220364231346 (describing how a family was able to learn more about their daughter's death by accessing her social media accounts).

As Naomi Cahn explains in her outstanding contribution to the *Vanderbilt Law Review*'s Symposium on the Role of Federal Law in Private Wealth Transfer,[4] these ISPs are concerned about a byzantine federal statute from 1986: the Stored Communications Act ("SCA"). Section 2701 of the SCA criminalizes unauthorized access to electronic communications,[5] presenting a seemingly nasty glitch for fiduciaries attempting to marshal a decedent's digital assets. Section 2702 bars ISPs from disclosing a customer's private data without her "lawful consent."[6] Noting that the SCA predates the rise of email—let alone the phenomenon of a valuable Twitter account—Professor Cahn argues that the statute should not govern fiduciaries.[7] Alternatively, assuming that the SCA does apply in the trusts and estates context, Professor Cahn discusses various ways around this obstacle, including the Uniform Law Commission's draft Fiduciary Access to Digital Assets Act ("FADA"), which would clarify that fiduciaries generally enjoy the "authorization"' and "lawful consent" necessary to acquire a decedent's online accounts.[8]

This short invited reply takes a different route to the same destination. It begins by offering a reading of the SCA that diverges slightly from Professor Cahn's. However, it uses that discussion to echo her critique of the SCA and bolster the case for the FADA.

II. THE SCA

The SCA is dusty and complex, and courts commonly disagree about the meaning of its key terms. Thus, although many commentators have noted that the statute "may" cast a shadow over the inheritability of digital assets, few have attempted to define its precise effect.[9] Professor Cahn deserves credit for filling this gap. As I

---

4. *See* Cahn, *supra* note 1.

5. 18 U.S.C. § 2701 (2012).

6. *Id.* at § 2702(a)(1)–(2).

7. *See* Cahn, *supra* note 1, at 1717–18 (arguing that the statute should not govern fiduciaries).

8. *See id.* at 21–24; UNIF. LAW COMM'N, FIDUCIARY ACCESS TO DIGITAL ASSETS ACT ("FADA") (2014), *available at* http://www.uniformlaws.org/shared/docs/ Fiduciary%20Access%20 to%20Digital%20Assets/2014mar_FADA_Mtg%20Draft.pdf, *archived at* http://perma.cc/K9Q5-UTNH (last visited May 7, 2014).

9. Sandi S. Varnado, *Your Digital Footprint at Death: An Illustration of Technology Leaving the Law Behind*, 74 LA. L. REV. 719, 749 (2014); *see also* James D. Lamm et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries From Managing Digital Property*, 68 U. MIAMI L. REV. 385, 404 (2014) (noting that "case law provides no clear answer regarding whether a fiduciary can provide 'lawful consent' to a service provider"); Kristina Sherry, Comment, *What Happens to Our Facebook Accounts When We Die?: Probate Versus Policy and the Fate of Social-Media Assets Postmortem*, 40 PEPP. L. REV. 185, 211 (2012)

discuss next, I partially agree with her claim that the SCA is less of a roadblock than commonly believed.

A. Section 2701

For fiduciaries, the most intimidating part of the SCA is section 2701. That provision levies criminal penalties upon anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or who "exceeds an authorization to access . . . and thereby obtains, alters, or prevents authorized access to a[n] . . . electronic communication while it is in electronic storage."[10] Congress intended this language to create a weapon against "computer hackers (e.g., electronic trespassers)."[11] But because the statutory text sweeps broadly and prohibits simply "logging onto another's email account without permission,"[12] scholars have voiced concern that fiduciaries may violate the SCA by taking control of a decedent's electronic assets.[13]

However, I share Professor Cahn's view that section 2701 does not apply to fiduciaries. For starters, the passage's key phrase—"without authorization"—is exceedingly narrow. "Authorization" means "power granted by authority," as several courts have recognized while interpreting the SCA's sister statute, the Computer Fraud and Abuse Act ("CFAA").[14] As a result, a decedent whose will or trust expressly allows a fiduciary to control her electronic possessions automatically authorizes access to those assets under section 2701.

To be sure, because few estate plans actually mention digital assets, the breadth of the term "authorization" does not get us very far. What happens when a decedent executes a testamentary instrument that is less specific? Does the bare act of naming an executor or trustee—arming someone with the generalized right to

---

(explaining that the SCA "may inhibit the probate process"); Molly Wilkens, Note, *Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?*, 62 HASTINGS. L.J. 1037, 1053 (2011) (noting that the SCA is "unclear" and "leave[s] questions of access after death largely unanswered").

10. 18 U.S.C. § 2701 (2012).

11. Lasco Foods, Inc. v. Hall and Shaw Sales, Mktg., & Consulting, LLC, 600 F. Supp. 2d 1045, 1049 (E.D. Mo. 2009).

12. *See* Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008) (noting that the statute prohibits logging on to another's computer but does not prohibit the use of information gained without permission).

13. *See* Lamm, *supra* note 9, at 399–402 (explaining that fiduciaries risk criminal liability for logging onto and managing a decedent's digital account under the CFAA, a statute similar to the SCA with a similarly broad scope and discussed *infra* text accompanying note 13).

14. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (quoting RANDOM HOUSE UNABRIDGED DICTIONARY 139 (2d ed. 2001)).

manage property—count as authorization to handle online accounts? What about intestacy, where a decedent has done nothing to make her wishes known?

For several reasons, I believe that fiduciaries in these contexts also enjoy authorization. First, section 2701's common law roots support this reading. As the Fourth Circuit has observed, Congress modeled section 2701 on the venerable doctrine of trespass to chattels.[15] A cause of action for trespass to chattels arises when a defendant damages an item or dispossesses its owner of it.[16] Of course, fiduciaries are nothing like these third-party tortfeasors. A fiduciary "steps into the decedent's shoes"[17] and wields "the same power over the title to property of the estate that an absolute owner would have."[18] Acting on the decedent's behalf—essentially acting *as* the decedent—a fiduciary can sell property, pay debts, settle claims, manage businesses,[19] and waive the attorney-client privilege.[20] It would be bizarre if a fiduciary, cloaked with this robust authority, committed a trespass-like offense simply by logging on to a decedent's accounts. Second, it need not be the *decedent* who authorizes access. Indeed, one only lacks authorization when one acts "without *any* permission."[21] As a result, authorization can arise from any legitimate conferral of rights, such as a probate court order giving an executor or administrator dominion over the estate.

Here I must add an asterisk. Some ISP terms of service ("TOS") prohibit users from transferring their accounts to others.[22] One might argue that this restrictive boilerplate makes fiduciary access unauthorized. However, I am not persuaded that TOS should affect the authorization analysis.[23] Such a reading would allow fine print to

---

15. *See* Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 208 (4th Cir. 2009) (noting that the SCA "closely mirrors" the doctrine of trespass to chattels); *cf.* Theofel v. Farey-Jones, 359 F.3d 1066, 1073 (9th Cir. 2004) (construing § 2701 in light of the doctrine of trespass to land).

16. RESTATEMENT (SECOND) OF TORTS § 218(b)–(c) (1965).

17. People v. Jessee, 165 Cal. Rptr. 3d 280, 286 (Ct. App. 2013).

18. UNIF. PROBATE CODE § 3-711 (2010).

19. *Id.* at § 3-715.

20. *See, e.g.*, *In re* DelGatto, 950 N.Y.S.2d 738 (N.Y. App. Div. 2012) (stating that the fiduciary waived the attorney-client privilege by challenging the validity of the trust and related documents).

21. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133, 1135 (9th Cir. 2009) (emphasis added).

22. *See, e.g.*, David Horton, *Indescendibility*, 102 CALIF. L. REV. 543, 567 (2014) (explaining restraints on a user's right to transfer).

23. Of course, fine print that denies decedents the right to convey electronic assets may not be valid under black-letter contract law. *See, e.g.*, Ajemian v. Yahoo!, Inc., 987 N.E.2d 604, 612–

define the scope of criminal liability. In turn, this would be perverse: indeed, "the mere breach of a contract is not 'unlawful' in a criminal sense."[24] This is particularly true for TOS: "private policies that are lengthy, opaque, subject to change and seldom read."[25]

Finally, even if courts interpret authorization narrowly, section 2701 is limited in several respects. For one, the provision governs unauthorized access to "a facility through which an electronic communication service is provided."[26] As several courts have recognized, a facility is an ISP's server—not an individual's personal computer, smart phone, or tablet.[27] Thus, if section 2701 does govern fiduciaries, it does not prevent them from acquiring assets from a decedent's hard drive or handheld device, such as photographs on an iPad or downloaded email attachments on a personal computer. Also, because section 2701 only forbids the access of data that is in "electronic storage,"[28] it should not cover a broad category of emails: those that have already been read. Congress defined "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[29] An unopened message in a recipient's in-box is "in 'temporary, intermediate storage.' "[30] Likewise, ISPs often clone their

---

13 (Mass. App. Ct. 2013) (refusing to enforce forum selection clause in browsewrap contract in dispute over indescendibility provision in Yahoo!'s TOS).

24. *In re* Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 557–60 (N.D. Tex. 2005) (discussing section 2702).

25. United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc) (discussing the analogous context of the CFAA); United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009) (reasoning that construing the CFAA to cover a defendant's breach of TOS would violate the void-for-vagueness doctrine); *see also* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1582 (2010) ("[N]o one actually treats TOS as if they govern access rights.").

26. 18 U.S.C. § 2701(a)(1) (2012).

27. *See, e.g.*, Garcia v. City of Laredo, Tex., 702 F.3d 788, 793 (5th Cir. 2012) ("[T]he statute envisions a *provider* (the ISP or other network service provider) and a *user* (the individual with an account with the provider), with the *user's communications in the possession of the provider*." (quoting Orin S. Kerr, *infra* note 30, at 1215)); United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1057–58 (N.D. Cal. 2012) (stating that a mobile device is not a "facility" within the statute); Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz, 793 F. Supp. 2d 311, 337 (D.D.C. 2011) (stating that a personal computer is not a "server"); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008).

28. 18 U.S.C. § 2701.

29. 18 U.S.C. § 2510(17) (incorporated by 18 U.S.C. § 2711(1)).

30. Rene v. G.F. Fishers, Inc., 817 F. Supp. 2d 1090, 1096 (S.D. Ind. 2011) (citing Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965, 987 (C.D. Cal. 2010) (quoting 18 U.S.C. § 2510(17)(A))).

servers as a fail-safe against equipment failure, thus generating duplicate emails that are kept "for backup purposes."[31] Conversely, once opened by recipients, emails are neither awaiting delivery (stored "temporar[ily]") nor copies preserved out of the ISP's abundance of caution.[32] Accordingly, fiduciaries should be able to click through a decedent's previously opened digital correspondence in much the same way they can sift through conventional letters.

In sum, section 2701 should not govern fiduciary access to a decedent's digital assets. But even if the provision does apply, it is riddled with holes. Decedents can exempt particular items by downloading them onto their personal computer or handheld device. Even simply clicking on an email should be enough to liberate it from the confines of section 2701.

B. Section 2702

Unfortunately, section 2702 is more problematic. That provision bars certain ISPs from disclosing the contents of digital accounts—such as emails, instant messages, or images—without the user's "lawful consent."[33] What is lawful consent? Professor Cahn and I agree that a decedent who drafts a testamentary instrument that explicitly allows her fiduciary to manage electronic assets has consented to disclosure. Similarly, customers should be able to take other steps that waive section 2702's protections. For instance, the

---

31. 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, 1216–18 & n.61 (2004).

32. *See, e.g.*, Roadlink Workforce Solutions, L.L.C. v. Malpass, No. 3:13-cv–05459-RBL, 2013 WL 5274812, at *4, (W.D. Wash. Sept. 18, 2013) (stating that emails that are "opened but not deleted" are not in storage); Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013) ("[E]-mails which the intended recipient has opened, but not deleted (and thus which remain available for later re-opening) are not being kept 'for the purposes of backup protection.' " (citation omitted)); *Crispin*, 717 F. Supp. 2d at 987 (indicating that once emails are opened, they are not awaiting delivery); United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (noting that the drafters of the statute intended to cover emails opened but left in the server); Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012) (holding that emails that have been opened but left on the server are not in electronic storage). Admittedly, there is contrary authority. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2003) ("[P]rior access is irrelevant to whether the messages at issue were in electronic storage."); Cheng v. Romo, No. Civ. A. 11-10007-DJC, 2013 WL 6814691, at *3 (D. Mass. Dec. 20, 2013) (concluding same). *But see* Kerr, *supra* note 31, at 1217 & n.61 (explaining why this conclusion is "implausible").

33. 18 U.S.C. § 2702(b)(3). Section 2702 does not apply to all ISPs. Instead, it only governs firms that offer services "to the public." *Id.* § 2702(a)(1)–(2); *see also* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998) (stating that defendants would be liable if they knowingly divulged information to the public). Because most commercial ISPs and social media sites are open to any willing customer, they are open "to the public" and therefore must contend with § 2702. However, educational and work-related email systems "are available only to users with special relationships with the provider." Kerr, *supra* note 31, at 1226.

House Report on the SCA emphasizes that users can satisfy the consent element by signing up for an ISP that permits disclosure:

> If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent on the part of a user to disclosures or uses consistent with those rules.[34]

Finally, customers can arguably consent in relatively casual ways. The legislative history also notes that "consent . . . need not take the form of a formal written document" and may flow from "action that evidences acquiescence to . . . disclosure or use."[35] Although this language is somewhat vague, it could extend to a situation in which an individual simply tells someone else that she wishes to convey her online accounts after she dies.

Nevertheless, decedents who do not fall into one of these camps probably have not consented to disclosure. Here I part ways with Professor Cahn, who construes consent and authorization as synonymous.[36] In my eyes, the critical difference is this: unlike authorization under section 2701, which a probate court can give, consent under section 2702 must stem from the *user*. Indeed, definitions of consent focus on the *consenting party*'s "[a]greement, approval, or permission as to some act or purpose."[37] Suppose a person neither signs up for an ISP that allows disclosure nor makes her wishes known, and then dies without a testamentary instrument that mentions digital assets. In the whistling silence of this scenario, no words or conduct give the ISP the green light to release the decedent's stored communications. True, consent is one of the slipperiest concepts in law and can be constructive or implied. Also, by making a will or trust, an owner passes the torch to her executor or trustee to manage her property after she dies. Likewise, even intestacy can represent a quasi-consensual state of affairs where, in lieu of creating an estate plan, a decedent "selects" a jurisdiction's off-the-rack distribution scheme. Yet the illustrations of consent in the SCA's legislative history involve affirmative conduct: forming a contract or making a statement that specifically bears on disclosure.[38]

---

34. H.R. REP. No. 99-647, at 66 (1986).

35. *Id.*

36. *See* Cahn, *supra* note 1, at 1717–18 (arguing that the statute should not govern fiduciaries).

37. BLACK'S LAW DICTIONARY 346 (9th ed. 2009).

38. There is a slightly stronger argument that fiduciaries can consent on behalf of a decedent for emails that a decedent has received, rather than written. Section 2702(b)(1) permits ISPs to disclose correspondence for which a user is an "addressee or intended recipient" to her "agent." If fiduciaries are a decedents' "agent[s]," then § 2702 does not govern messages sent by others to decedents.

Moreover, TOS have more bite under section 2702 than they do under section 2701. First, these provisions may allow section 2702 to override a decedent's attempt to convey digital assets. Suppose a customer signs a will that expressly leaves the contents of her email account to her spouse, but her ISP's TOS forbids posthumous conveyance. There is a plausible argument that she has consented, but is not acting lawfully. Admittedly, some authority suggests that simply breaching a contract "is not unlawful."[39] But at the same time, "[t]he plain and ordinary meaning of 'lawful' is that which is 'permitted by law,' "[40] and flouting a binding agreement does not seem to meet that standard. Also, allowing TOS to define authorization under section 2701 predicates criminal sanctions on a user's disregard of inconspicuous print, to rather harsh effect.[41] But because section 2702 only creates civil liability, no such concerns are present. Second, even if restrictive TOS do not affect section 2702's scope, they are a separate and independent basis for ISPs to resist disclosure. Section 2702 is a one-way street. If it governs, ISPs cannot release a subscriber's electronic correspondence. However, if section 2702 does not apply, the statute merely *permits*—but does mandate—disclosure.[42] Accordingly, a fiduciary seeking electronic property in the teeth of TOS must not only overcome section 2702 but also convince a court that the noninheritability clause is invalid under black-letter contract law.

To summarize, section 2702 creates a heavy default rule that emails and their ilk are indescendible. To escape the statute's strong gravitational pull, a fiduciary must show that a decedent actively agreed to convey her digital assets. And even that may not be enough if the ISP's TOS denies the power of posthumous transfer.

---

39. Benderson Dev. Co. v. U.S. Postal Serv., 998 F.2d 959, 962 (Fed. Cir. 1993) ("To breach a contract is not unlawful; the breach only begets a remedy in law or in equity."); *cf. In re* Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 560–61 (N.D. Tex. 2005) (holding that an airline did not violate § 2702 by disclosing customers' information even though doing so may have violated its own privacy policy).

40. Coats v. Dish Network, L.L.C., 303 P.3d 147, 150 (Colo. App. 2013) (quoting BLACK'S LAW DICTIONARY, *supra* note 37, at 965).

41. *See* United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012) (en banc) (describing violations of service agreements and criminal sanctions that could occur and a lack of public awareness).

42. For instance, the statute carves out "[e]xceptions for disclosure" in which "[a] provider . . . *may* divulge the contents of a communication." § 2702(b) (emphasis added).

III. THE FADA

The FADA makes digital assets presumptively inheritable.[43] The draft statute provides that fiduciaries are authorized users under section 2701 and "have the lawful consent of the account holder" for the purposes of section 2702.[44] In addition, unlike section 2702's regime of permissive disclosure, the FADA *requires* ISPs to divulge stored data to fiduciaries who have a decedent's blessing.[45] The FADA also takes a somewhat dim view of clauses in TOS that prohibit fiduciary access, invalidating them unless they are separately signed.[46] And finally, the FADA permits privacy-conscious testators to override the default and declare in their wills that their electronic property is indescendible.[47]

To see why these are sensible reforms, it is helpful to step back and examine the law's traditionally blunt policy toward inheritability. Generally, if you own something at death, you *must* convey it to someone else.[48] However, a small group of assets defies the irresistible magnetism of inheritance. Consider human body parts, which can be worth hundreds of thousands of dollars but cannot be transmitted by will, trust, or intestacy.[49] There are several rationales for this prohibition, but the critical one for my purposes is that some owners would *want* to exclude their biological material from their estate. Indeed, although many individuals would welcome the opportunity to

---

43. On its face, the draft statute accomplishes the more modest goal of facilitating fiduciary *access* without "vary[ing] the underlying laws of management, descent, and distribution that otherwise apply to all assets and property." Suzanne B. Walsh, *Coming Soon to a Legislature Near You: Comprehensive State Law Governing Fiduciary Access to Digital Assets*, 8 CHARLESTON L. REV. 429, 441–42 (2014). Yet I do not see a sharp distinction between allowing fiduciaries to control digital property and making digital property prima facie descendible. Assets are inheritable unless there is a roadblock like the SCA. Taking the SCA out of the equation thus places the onus on decedents to opt out of descendibility, either in their testamentary instruments or through TOS.

44. *See* FADA § 8(a)(2)–(3). As Professor Cahn notes, whether states have the power to define "authorization" and "lawful consent" within the meaning of the SCA raises a thorny preemption issue. *See* Cahn, *supra* note 1, at 1723–25 (noting that existing state laws and the UFADA expressly allow fiduciary access and define "lawful consent," causing a potential conflict with federal law).

45. *See* FADA § 9 (stating the procedures the government must follow to compel disclosure from ISPs).

46. *Id.* at § 8(b)–(c).

47. *See id.* at § 4 (giving fiduciaries authority over digital property "[u]nless prohibited by the will of a decedent").

48. *See* Horton, *supra* note 22, at 548–49 ("[O]wning an item confers the power to transfer it when one dies.").

49. *See id.* at 552–57 (noting that a deceased cannot leave her cadaver to her loved ones upon death).

expand the size of their legacies, others would object to the harvesting and sale of their organs on moral or ethical grounds. Accordingly, as I have discussed elsewhere, if policymakers decided to make human tissues descendible, they would also need to create a unique rule permitting owners to opt out.[50]

Similarly, not everyone would want to convey their electronic assets to others after death. Of course, the Internet has become a rich repository of memories, overflowing with pictures and conversations. Many people would gladly entrust this colorful digital scrapbook to future generations. Likewise, in this era of online banking and bill payment, it can be difficult to perform the nuts and bolts of estate administration without access to a decedent's in-box. Nevertheless, treating online belongings like all other property would raise grave privacy concerns. After all, "[e]ach of us can think of at least one e-mail that we would not want to fall into the wrong hands."[51] Indeed, there are numerous anecdotes of family members unearthing material that no decedent would want exposed.[52] As a mother remarked after discovering her deceased daughter's secret blog, "[s]he had passwords for a reason."[53]

Thus, digital assets should neither be completely descendible nor fully indescendible. Instead, the law should encourage users to make their posthumous wishes known on an account-by-account basis.

The SCA does not accomplish this goal. For one, the statute has the potential to thwart a decedent's intent. Recall that section 2702 may allow nontransferability provisions in TOS to override a testator or settlor's unambiguous attempt to bequeath digital assets. Only customers who sign up for the rare ISP that allows disclosure can be sure that their loved ones will receive their online belongings. This privileging of fine print over the commands of a decedent's will or trust is exactly backwards.

Moreover, the SCA gets the pivotal policy question—the choice of gap-filler—wrong. People often die without expressing their testamentary desires about digital assets. This makes the choice of default rule tremendously important. Should we adhere to the SCA and deem electronic property to be presumptively indescendible? Or

---

50. *See id.* at 587–88 (stating that an "all-out" descendibility with no opt-out provision would be unfair).

51. Justin Atwater, *Who Owns E-mail? Do You Have the Right to Decide the Disposition of Your Private Digital Life?*, 2006 UTAH L. REV. 397, 399.

52. *See, e.g.*, Fowler, *supra* note 3 (explaining that the decedent may not have wanted her personal information discovered).

53. *Id.* The blog was entitled "you wouldn't want to know." *Id.*

should we follow the FADA and make online belongings inheritable unless an owner tells us otherwise?

For several reasons, the FADA's approach is superior. First, as noted above, almost all property is descendible. Because emails and pictures embody a user's labor and ingenuity—two hallmarks of ownership[54]—most users probably believe that the same principle governs their online possessions. In turn, this makes a default rule of inheritability consistent with majoritarian expectations. Second, in other contexts, the values that the SCA safeguards during life dissipate upon death. Indeed, a personal representative cannot sue for posthumous invasion of a decedent's privacy or reputation.[55] It would therefore be anomalous to give the dead robust legal protections against embarrassment and other dignitary harms. And finally, societal interests tip the scales toward making electronic property generally inheritable. It would be tragic if "digital artifacts" died along with their creators, rather than leaving a vivid residue of life in the twenty-first century.[56]

IV. CONCLUSION

Professor Cahn's thoughtful Symposium piece fortifies her reputation as the leading scholar on digital inheritance. Although I interpret the SCA slightly differently, I agree that the FADA constitutes a huge upgrade from an outmoded federal law that was never meant to bully its way into the field of decedents' estates.

---

54. *See, e.g.*, Horton, *supra* note 21, at 567 ("Individuals often feel that the effort they have sunk into these things entitles them to the full panoply of property-style privileges.").

55. *See, e.g.*, *id.* at 560 (explaining there is no cause of action for slander or libel of a dead person).

56. *See, e.g.*, Deven R. Desai, *Property, Persona, and Preservation*, 81 TEMP. L. REV. 67, 89–93 (2008) ("Historians require access to primary sources to gain insight into how society has evolved.").