NORTHEASTERN UNIVERSITY
LAW REVIEW

Extra Legal

Life Beyond the Profile: What Happens to One's Assets After Digital Death?

By Diandra Franks[*]

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[1]

I. Introduction

In our current Information Age in which so much time is spent behind the surface of a screen, an enormous and ever-increasing amount of one's assets are stored within the confines of the World Wide Web. Whether or not the online asset is sentimental or financial, these accounts (social media, email, cryptocurrency, etc.) require users to create complicated, case-sensitive passwords as protection. This practice begs questions:

[*] Candidate for Juris Doctor, 2019, Northeastern University School of Law.

[1] U.S. CONST. amend. IV.

What happens to online accounts when someone dies? Should friends and heirs be allowed to breach traditional notions of privacy to preserve a loved one's memory?

Before the world was lived so predominantly behind screens, "estate planning and the administration of a decedent's estate was typically a process that focused on the individual's tangible belongings, financial assets, and real estate."[2] In this Information Age, "where almost every aspect of our lives is in some manner affected or controlled by information that is stored in an electronic form, it is not surprising that the impact of 'digital assets' has fundamentally and irrevocably changed the nature of estate planning and administration."[3] This paper explores the tension between traditional notions of privacy during a time when so much of one's life is willingly exposed online. In order to understand the state of the controversy, I will begin with a brief overview of the development of the right of privacy in America and then delve into popular types of digital assets in the world today. I will then discuss the legal implications of state and federal regulations regarding privacy rights associated with different online assets, and suggest solutions for practitioners preparing for their clients' digital deaths.

II. Right to Privacy

A right to privacy is not expressly granted in the Federal Constitution, but the United States Supreme Court has long recognized the existence of "zones of privacy" into which the government may only intrude upon a demonstration of a compelling state interest and by the least intrusive

[2] Michael D. Walker, *The New Uniform Digital Assets Law: Estate Planning and Administration in the Information Age*, 52 REAL PROP., TR. AND EST. L.J. 51, 52 (2017).

[3] *Id.*

means possible.[4] The Supreme Court first introduced the substantive privacy doctrine in *Griswold v. Connecticut*,[5] in which the Court stated that the right to privacy was found in "penumbras" that are given "life and substance" by the Bill of Rights.[6] The Court remarked that the First, Third, Fourth, Fifth, and Ninth Amendments combine to form "zone[s] of privacy."[7] These "zones of privacy" include matters relating to: marriage, procreation, contraception, familial relationships, child rearing, and education.[8] Ultimately, the Court determined that the Due Process Clause of the Fourteenth Amendment guaranteed such privacy rights—a legal theory Justice Harlan initially advanced in his *Griswald* concurrence."[9] Courts have since determined that the "zones of privacy" implicate two separate privacy interests: 1) the "individual interest in avoiding disclosure of personal matters;"[10] and 2) "the interest in independence in making certain kinds of important decisions."[11]

The Ninth Amendment is often cited for the notion that not all rights protected by the Constitution are specifically enumerated: "[t]he

---

[4] JOHN F. ADKINS ET AL., MASS. PRACTICE SERIES, 45 Employment Law § 10.3 (3d. ed. 2018).

[5] Griswold v. Connecticut, 381 U.S. 479 (1965).

[6] *Id.* at 484.

[7] *Id.* at 484–85.

[8] *See* Lawrence v. Texas, 539 U.S. 558 (2003) (sexual intimacy between same-sex couples); Bellotti v. Baird, 443 U.S. 622 (1979) (abortion rights); Moore v. City of East Cleveland, 431 U.S. 494 (1977) (familial relationships); Pierce v. Soc'y of the Sisters of the Holy Names of Jesus and Mary, 268 U.S. 510, 535 (1925) (childrearing and education); Skinner v. Oklahoma *ex rel.* Williamson, 316 U.S. 535 (1942) (procreation); Loving v. Virginia, 388 U.S. 1 (1967) (marriage).

[9] Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1393–94 (1992); *see* Griswold, 381 U.S. at 500 (Harlan, J., concurring).

[10] Whalen v. Roe, 429 U.S. 589, 589–99 (1977).

[11] *Id.* at 599-600.

enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[12] In 1965, the Supreme Court announced privacy as a fundamental right protected by the Constitution,[13] and many cases since have expanded on the right to privacy doctrine.[14] Its exact parameters remain ill-defined, and it is time for more guidance concerning an individual's privacy rights in his or her digital assets.

While scholars may disagree about the meaning of the right to privacy and all that it encompasses, "the protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."[15] Individual states and the federal government need to take a more active role in defining privacy rights for digital assets, especially considering the popularity and variety of digital assets in the world today.

III. Types of Digital Assets

To conceptualize the difficulty and necessity in regulating this area, it is important to understand the types of digital assets. The Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA"), which revised the 2014 Uniform Fiduciary Access to Digital Access Act ("UFADAA") and greatly reduces the authority of an executor to access

---

[12] Joseph F. Kadlec, *Employing the Ninth Amendment to Supplement Substantive Due Process: Recognizing the History of the Ninth Amendment and the Existence of Nonfundamental Unenumerated Rights*, 48 B.C. L. REV. 387, 388–89 (2007); U.S. CONST. amend. IX.

[13] *Griswold*, 381 U.S. at 485.

[14] *See, e.g.*, Moore v. City of E. Cleveland, 431 U.S. 494 (1977); Roe v. Wade, 410 U.S. 113 (1973); Eisenstadt v. Baird, 405 U.S. 438 (1972); Loving v. Virginia, 388 U.S. 1 (1967).

[15] Katz v. United States, 389 U.S. 347, 350–51 (emphasis omitted).

digital assets, provides beneficial definitions that aid conceptualization. [16] RUFADAA defines "digital asset" as "an electronic record in which an individual has a right or interest."[17] This definition "does not include the underlying asset or liability unless the asset or liability is itself an electronic record."[18] A "record" includes "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[19] "Electronic" is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities."[20] The "definition of digital assets refers to an electronic record that is owned by an 'individual.'"[21] Therefore, "this definition would appear to exclude any digital asset that is owned by an estate or business entity, all of which *are* included within RUFADAA's separate definition of a 'person.'"[22]

Evan Carroll, co-founder of "The Digital Beyond blog" "identifies two categories of digital assets: (1) those stored locally, on tangible electronic devices a person owns, and (2) those stored elsewhere on devices accessed by contract with the device owner."[23] Carroll then breaks these two sub-groups of digital assets into five separate categories: (1) "devices

---

[16] Walker, *supra* note 2, at 59.

[17] *See* REVISED UNIF. FIDUCIARY ACCESS TO DIG. ASSETS ACT § 2(10) (UNIF. LAW COMM'N 2015).

[18] *Id.*

[19] *Id.* § 2(22).

[20] *Id.* § 2(11).

[21] Walker, *supra* note 2, at 53; *see also* REVISED UNIF. FIDUCIARY ACCESS TO DIG. ASSETS ACT § 2(10) (UNIF. LAW COMM'N 2015).

[22] Walker, *supra* note 2, at 53; *see also* REVISED UNIF. FIDUCIARY ACCESS TO DIG. ASSETS ACT § 2(17) (UNIF. LAW COMM'N 2015).

[23] Kristina Sherry, *What Happens to our Facebook Accounts When We Die?: Probate Versus Policy and the Fate of Social-Media Assets Postmortem*, 40 PEPP. L. REV. 185, 194 (2012); *see also* THE DIGITAL BEYOND, http://www.thedigitalbeyond.com/ (last visited July 16, 2018).

and data," (2) "electronic mail (e-mail)," (3) "online accounts," (4) "financial accounts," and (5) "online businesses."[24] I will discuss three popular types of digital assets: 1) social media accounts, 2) email accounts, and 3) cryptocurrency accounts.

a. Social Media Accounts

Unfortunately, the right to privacy pre-dates modern technology. Today, like never before, personal information is given freely, openly, and frequently in the ever-growing online American market.[25] With the expansion of internet use into online social media platforms where people openly expose private information and photographs to "friends" and "followers," individuals risk losing valuable memories and sentimental images of loved ones upon death. These online social media accounts, or digital assets, have "no extrinsic economic value, but may have tremendous sentimental value."[26] Alternatively, internet users risk the possibility that family members or heirs may access intimate communications without the consent of the decedent.

Concern over online privacy has grown from 43% being "very concerned" and 35% being "somewhat concerned" about threats to their personal privacy in 1990,[27] to upwards of 88% of 1,500 internet users being concerned about website collection of personal information in

---

[24] *Id.* at 195.

[25] In 2005, total e-commerce sales in the United States were estimated at $86.3 billion, an increase of 24.6% from 2004. These online sales accounted for 2.3% of total sales in the country, up from 2.0% of total sales in 2004. *Quarterly Retail E-Commerce Sales: 4th Quarter 2005*, U.S. CENSUS BUREAU (U.S. Dep't of Commerce, D.C.), Feb. 17, 2006.

[26] Walker, *supra* note 2, at 54.

[27] *Public Opinion on Privacy*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/survey/# (last visited Apr. 17, 2019) (citing *The Harris Poll*, No. 892049 (Jan. 1990)).

2003.[28] A more recent survey in 2014 found that "80% of social media users said they were concerned about advertisers and businesses accessing the data they share on social media platforms, and 64% said the government should do more to regulate advertisers."[29] Acknowledging the fact that Facebook users will inevitably pass away while still having active accounts, Facebook implemented a "memorializing" feature in 2009, "allowing friends and families to request that a decedent's account become effectively frozen amid efforts to avoid awkward invitations to 'connect' with dead people or 'tag' them in photos."[30] This response, while beneficial for family members and loved ones, does not take into account how long a memorialized presence should last, or whether or not the Facebook user would have wanted his or her page memorialized for any period of time at all. Probate and intestacy laws' relevance to social media is complicated by the fact that the "property" status of social media accounts remains unclear.[31]

b. Email Accounts

The Massachusetts Supreme Judicial Court ("SJC") recently considered this tension over access to a loved one's digital assets in

---

[28] Anne Kandra & Andrew Brandt, *Great American Privacy Makeover*, PCWORLD (Oct. 8, 2003, 4:00 PM), https://www.pcworld.com/article/112468/article.html.

[29] Lee Rainie, *Americans' complicated feelings about social media in an era of privacy concerns*, PEW RESEARCH CENTER (last visited Apr. 12, 2019), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[30] Sherry, *supra* note 23, at 187; *see also* Matthew Moore, *Facebook Introduces 'Memorial' Pages to Prevent Alerts About Dead Members*, THE TELEGRAPH (Oct. 27, 2009, 10:59 AM), http:// www.telegraph.co.uk/technology/facebook/6445152/Facebook-introduces-memorial-pages-to-prevent-alerts-about-dead-members.html (explaining Facebook's decision to allow friends and family to contact the company and request to "memorialize" deceased members' pages).

[31] *See generally* John Connor, *Digital Life After Death: The Issue of Planning for a Person's Digital Assets After Death*, 3 EST. PLAN. & COMMUNITY PROP. L.J. 301 (2011).

Ajemian v. Yahoo!, Inc.[32] Here, the court considered whether the Stored Communications Act ("SCA") protected a deceased person's right to privacy in digital assets where the decedent's siblings and personal representatives sought to access the contents of their brother's Yahoo email account upon his sudden death.[33] In this case of first impression, the SJC was "called upon to determine whether the SCA prohibits Yahoo from voluntarily disclosing the contents of the e-mail account to the personal representatives of the decedent's estate."[34] Yahoo argued that, under the SCA, lawful consent could only come from the decedent, who was the original user of the email account.[35] The court held that "federal law, specifically the [SCA], does not prohibit an email service provider from disclosing email content to a decedent's personal representative."[36]

This ruling is incredibly current and "significant to the fiduciary community in Massachusetts because it helps define post mortem ownership of digital assets."[37] "Congress enacted the SCA in 1986 'to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.'"[38] The SCA, "subject to certain exceptions," "prohibits unauthorized third parties from accessing communications stored by

---

[32] 84 N.E.3d 766 (Mass. 2017).

[33] *Id.* at 768.

[34] *Id.*

[35] Colin Korzec & Mary H. Schmidt, *The Internet and the Afterlife*, 62 BOS. B.J. 13, 14 (2018).

[36] *Id.* at 13.

[37] *Id.*

[38] *Ajemian,* 84 N.E.3d at 771; The Stored Communications Act (SCA) was enacted as Title II of the broader Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

service providers," "regulates when service providers voluntarily may disclose stored electronic communications," and "prescribes when and how a government entity may compel a service provider to release stored communications to it."[39] The SJC concluded that the SCA does not prohibit the disclosure of the contents of an email account, but "[r]ather, it permits Yahoo to divulge the contents of the e-mail account where, as here, the personal representatives lawfully consent to disclosure on the decedent's behalf."[40]

c. Cryptocurrency Accounts

While some statutes have been enacted at the state and federal levels regarding digital assets, the rise in popularity of cryptocurrencies demonstrates the need for even stronger and more concrete regulations in this online market. Cryptocurrencies have been defined as "web-based, peer-to-peer payment systems that rely on cryptography."[41] This form of currency functions as "a digital unit of exchange that is not backed by a government-issued legal tender."[42] Cryptocurrencies "are computer files tendered as a form of payment for *real* goods and services."[43] "Cryptocurrencies are created by mining," which is essentially "solving

[39] *See* Stored Communications Act, 18 U.S.C. §§ 2701–2703 (2012); *Ajemian*, 84 N.E.3d at 771.

[40] *Ajemian*, 84 N.E.3d at 768.

[41] Omri Y. Marian, *Are Cryptocurrencies 'Super' Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 41 (2013).

[42] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-13-516, VIRTUAL ECONOMIES AND CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX COMPLIANCE RISKS (2013); Marian, *supra* note 41, at 41.

[43] Marian, *supra* note 41, at 41.

automatically generated mathematical puzzles."[44] Mining may be defined as "the competitive process of collecting transactions and adding them to the blockchain in the form of blocks."[45] "Blockchain is a sequence of blocks, which holds the complete record of transactions (a public ledger) indicating the order in which the transaction occurred."[46]

Bitcoin, created by a person/group identified pseudonymously as Satoshi Nakamoto, is the most dominant cryptocurrency and started the trend towards utilizing and investing in cryptocurrency.[47] The appeal of bitcoin and other cryptocurrencies is that they eliminate the middleman and allow "online payments to be sent directly from one party to another without going through a financial institution."[48] The creation of bitcoin coincided with the 2008 global financial crisis, so it is frequently suggested that bitcoin is a direct result of citizen distrust in government institutions and banks.[49] Because the mining system is run by a decentralized network of computers and not by a single company or person, people instilled trust in bitcoin.[50] Bitcoin records are stored on every computer, including balances and transactions.[51] This storage helps

---

[44] Dr. Asress Adimi Gikay, *Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons from European Union Law*, 9 CASE W. RESERVE J.L. TECH & INTERNET 1, 4 (2018).

[45] *Id.*

[46] *Id.*

[47] *See generally* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (Nov. 1, 2008), https://bitcoin.org/bitcoin.pdf.

[48] *Id.*

[49] *See, e.g.*, Yanis Varoufakis, *Bitcoin and the Dangerous Fantasy of 'Apolitical' Money*, YANIS VAROUFAKIS BLOG (Apr. 22, 2013), https://www.yanisvaroufakis.eu/2013/04/22/bitcoin-and-the-dangerous-fantasy-of-apolitical-money/.

[50] Nathaniel Popper, *What Is Bitcoin, and How Does It Work?*, N.Y. TIMES, Oct. 1, 2017, at 1.

[51] *Id.*

"maintain the network—about 9,500 computers in late 2017."[52] Cryptocurrencies have many potential advantages over cash money that justify their creation: they can be cheap payment methods, and are trustworthy, decentralized, and anonymous.[53] Additionally, cryptocurrencies eliminate expensive transaction fees (with no middleman),[54] are faster because there is no need for verification of available funds by a bank,[55] and protect merchants against disputed or fraudulent chargebacks (due to the irreversibility of the transactions).[56]

IV. Current State and Federal Regulations

Many view the right to privacy as encompassing the right to have personal information remain undisclosed unless otherwise granted.[57] Some states are starting to recognize the problems posed by the uncertainty regarding privacy rights in digital death.[58] Additionally, some legislation has passed at the federal level in order to deal with the impact of internet communications. As stated previously, Congress passed the SCA in 1986 as part of the Electronic Communications Privacy Act in order to deal with the impact of internet communications on privacy

[52] *Id.*

[53] *See* Ignacio Mas & David Lee Kuo Chen, *Bitcoin-Like Protocols and Innovations*, in HANDBOOK OF DIGITAL CURRENCY: BITCOIN, INNOVATION, FINANCIAL INSTRUMENTS, AND BIG DATA 417, 436 (David Lee Kuo Chuen ed., 2015).

[54] *See* JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 10, 14, 22–23 (2d ed. 2013), https://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.3.pdf.

[55] *Id.*

[56] *Id.* at 12, 15.

[57] *See* Sterling v. Borough of Minersville, 232 F.3d 190, 195 (3d Cir. 2000); Gruenke v. Seip, 225 F.3d 290, 303–04 (3d Cir. 2000); Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1139–40 (3d Cir. 1995); Fraternal Order of Police v. City of Philadelphia, 812 F.2d 105, 110 (3d Cir. 1987); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577–78 (3d Cir. 1980).

[58] Sherry, *supra* note 23, at 216 (citing Connecticut, Rhode Island, Indiana, Oklahoma, and Idaho as examples of states with statutes that concern digital assets).

concerns posited by the Fourth Amendment. In 1986, Congress also passed the Computer Fraud and Abuse Act (CFAA) to impose both criminal and civil liability upon anyone who "intentionally accesses a computer without authorization or exceeds authorized access" and obtains information from any "protected computer."[59]

Additionally, all 50 states have statutes criminalizing "unauthorized access" or "hacking" of computers/computer systems.[60] Determination of whether a fiduciary possesses legal authority for the purpose of the CFAA and state counterparts depends on two questions: 1) "[d]oes the fiduciary have clear legal authority to access the computer or digital assets of the decedent or incapacitated individual?;" and 2) "[i]f the computer system or digital asset is subject to the terms and conditions of a [Term of Service Agreement] TOSA, does the fiduciary's access violate the terms of that TOSA?"[61] Even "a fiduciary with ostensible legal authority may still violate the CFAA if the fiduciary's access violates the terms of the TOSA."[62]

The "original" UFADAA was approved in 2014 and subsequently introduced in approximately 27 states.[63] UFADAA, however, nearly

---

[59] 18 U.S.C. § 1030(a)(2)(C) (1984). For purposes of the CFAA, a "protected computer" is defined in 18 U.S.C. § 1030(e)(2) as a computer exclusively for the use of affecting the "use of a financial institution or the United States Government," or "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

[60] *Computer Crime Statutes*, NAT'L CONF. OF STATE LEGIS. (May 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

[61] Walker, *supra* note 2, at 57.

[62] *Id.*

[63] *See* Robert K. Kirkland, *Pixar for Estate Planners: Who Gets Your Digital Stuff When You've Logged Off for the Final Time*, AM. LAW INST., Sept. 13, 2016, at 27.

completely failed, and "representatives from the [Uniform Law Commission] and the digital provider industry entered into negotiations to discuss a compromise, the result of which was RUFADAA."[64] The final draft was formally approved in July 2015, and "[u]nlike the original UFADAA, which granted fiduciaries *presumptive* authority to access digital assets, RUFADAA places great emphasis upon whether the deceased or incapacitated user *expressly* consented to the disclosure of the content of the digital assets."[65] This *express* consent could be granted through "an 'online tool' or an express grant of authority in the user's estate planning documents or power of attorney."[66] In this manner, "RUFADAA respects the concept of 'lawful consent' under the SCA, and, unlike UFADAA, does not attempt to impute such lawful consent to the fiduciary."[67]

V. What Can Practitioners Do?

While a country full of booming technology is praised for advancing its citizens at rapid rates, it creates problems in a legal system that can be slow to progress. In regards to virtual currency and cryptocurrency, individuals should push the legislature to develop more useful regulations for dealing with these digital assets upon death. Developments in this realm have included clarification of cryptocurrency's treatment under the Bank Secrecy Act (BSA),[68] state

[64] Walker, *supra* note 2, at 59.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *See* U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013).

money transmitter laws,[69] federal securities laws,[70] and federal tax laws.[71] While these regulations are important and necessary, more needs to be done.

When it comes to cryptocurrency accounts, for example, the lack of a middleman may appease citizen distrust of government institutions and banks, but "[c]utting out the middleman (such as a bank or investment firm) by using this new platform might just leave a hole in the ability to identify [one's] ownership of crypto assets at [their] death."[72] If one invests in cryptocurrency but does not discuss this investment with their family and does not update his or her will to indicate the disposal of such assets, the account is likely to remain hidden upon death and forever thereafter. Unlike traditional assets, "no account statements are issued for cryptocurrency accounts."[73]

To prevent this lack of discovery from occurring, without any current

---

[69] *See, e.g.*, KAN. OFFICE OF THE STATE BANK COMM'R, MT 2014-01, REGULATORY TREATMENT OF VIRTUAL CURRENCIES UNDER THE KANSAS MONEY TRANSMITTER ACT (2014), http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf; Memorandum from Charles G. Cooper, Banking Comm'r, Texas Dep't of Banking, to All Virtual Currency Cos. Operating or Desiring to Operate in Tex. (Jan. 2, 2019), http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf; Memorandum from Deborah Bortner, Director, Dep't of Fin. Insts. Div. of Consumer Servs., to Virtual Currency Cos. Operating or Wishing to Operate in Wash. State (Dec. 8, 2014), http://www.dfi.wa.gov/documents/money-transmitters/virtual-currency-interim-guidance.pdf.

[70] *See* SEC v. Shavers, No. 4:13-cv-416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013) (holding that Bitcoin investments are securities under federal securities law).

[71] *See* I.R.S. Notice 2014-21, 2014-16 I.R.B. 938.

[72] Mary Ford, *What happens to your cryptocurrency when you die?*, NIXON PEABODY TRUSTS AND ESTATES BLOG, (May 25, 2018), http://web20.nixonpeabody.com/trusts/Pages/Trusts-And-Estates.aspx?ID=297&Title=What+happens+to+your+cryptocurrency+when+you+die?+.

[73] *Id.*

regulations in this specific area, owners of crypto assets "should prepare, and maintain, an inventory of crypto-asset accounts and the exchanges used, including account login, password and private key information" and keep this information "in a secure location."[74] Some cryptocurrency owners may utilize cryptocurrency wallets to hold their digital currency. These cryptocurrency wallets can hold hundreds of digital currencies,[75] and keep track of balances and crucial details, such as "when, where and how much you spent, added or withdrew."[76] These wallets "may be online, mobile, desktop, hardware, paper or a combination of these types."[77] "Each wallet has a unique protocol used to gain access to its contents."[78] The wallets essentially function as safety deposit boxes, guarded by "private keys or master keys," which are digital keys that take the form of hexadecimal codes.[79] These codes are long, so it is important to write them down and keep them safely stored.[80] Because the private key is needed to access assets and to authorize transfers from the wallet,[81] the assets could be lost forever if a user has not relayed the code to a loved one before his or her death. Even if the existence of a crypto asset is known, the heir may need to know the cryptocurrency wallet information to access the currency. For this reason, executors not only need to know

---

[74] *Id.*

[75] Crowdwiz, *How Does A Cryptocurrency Wallet Work and How to Create One*, Medium (Nov. 1, 2017), https://medium.com/@Crowdwiz.io/how-does-a-cryptocurrency-wallet-work-and-how-to-create-one-f234c6ec076f.

[76] *See id.*

[77] Ford, *supra* note 72, at 1.

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

of the existence of crypto assets, but they also need to know how to access any potential cryptocurrency wallets.[82]

Regarding other digital assets, such as social media and email accounts, the law is thankfully developing, though at slow rates compared to how quickly technology and life online is expanding. "Under the current rubric of federal and state laws, including RUFADAA and its inherent deference to the 'lawful consent' requirements of the SCA, the most important step [for practitioners to take] in the process of planning is to include a clear expression of such 'lawful consent' in the individual's applicable estate planning documents."[83] Absent this "clear expression of a user's consent, the fiduciary will not be able to access the content within the digital asset and may be limited to a 'catalogue' of electronic communications."[84] The "catalogue [of] information" can be "helpful" for the "personal representative in administering the estate" and ascertaining what is in the estate, but without access to the content within, this "catalogue could potentially raise more questions than it answers."[85] Provisions should be adapted to wills or estate plans in order to properly grant digital asset access authority to heirs, trustees, beneficiaries, etc.

Until the law becomes more comprehensive, practitioners should keep many elements in mind. First, individuals should "clearly express" consent to "disclosure to the fiduciary of the *content* of any digital asset" to invoke "the 'lawful consent' provision of the SCA."[86]To try to avoid any

---

[82] *Id.*

[83] Walker, *supra* note 2, at 68.

[84] *Id.*

[85] *Id.*

[86] 18 U.S.C. § 2702(b)(3) (2018); Walker, *supra* note 2, at 68.

issues in whether or not the SCA consent provision has been satisfied, "it is best to cite the SCA and the CFAA in the provision."[87] Next, "the provision should give the fiduciary the authority to access a digital asset in any location, whether it is stored on a tangible digital device (such as a personal computer or memory drive) or at an Internet location."[88] Thirdly, "the provision should give the fiduciary the authority to hire a 'technical' expert or consultant to help the fiduciary access the content of a digital asset or possibly secure the integrity and security of an electronic device or online account."[89] Finally, "the provision should clearly state that the fiduciary is an 'authorized user' for purposes of applicable computer-fraud and unauthorized-computer-access laws, such as the CFAA."[90] Basically, practitioners should "attempt to delineate an intentional process for dealing with a client's digital assets."[91]

As the law surrounding digital assets is likely to be further supplemented in the future, "careful application of existing fiduciary standards will likely be helpful," in an estate or trust administration.[92] A fiduciary's duty of care is often expressed as a "prudent person" standard: "[a] trustee shall administer the trust as a prudent person would, by considering the purposes, terms, distributional requirements, and other circumstances of the trust."[93] The Restatement recommends a trustee exercise an "external standard" of care and skill when handling the digital

[87] Walker, *supra* note 2, at 68.

[88] *Id.*

[89] *Id.*

[90] *Id.* at 69.

[91] *Id.*

[92] *Id.* at 70.

[93] *Id.*; UNIF. TRUST CODE § 804 (UNIF. LAW COMM'N, amended 2010).

assets held by an estate or trust."[94] Under this standard, the trustee "must evolve to meet the changing manner in which individuals own and manage their assets."[95] With the expansion of digital assets, practitioners need to evolve to meet the changing needs of their clients.

If decedents do not plan for "digital death" adequately, fiduciaries must still engage in "prudent" action.[96] Examples of engaging in prudent action include: "hir[ing] a forensic expert in information technologies to advise the fiduciary on a prudent process for locating a decedent's digital assets," "determin[ing] whether it is possible to gain working access to important 'portals' into the decedent's digital existence," and consulting "tax returns and Forms 1099" to "reflect assets that might not otherwise be found in traditional 'paper records' such as account statements."[97] These types of measures can be taken to supplement the lack of concrete and expansive law in this area.

VI. Conclusion

United States citizens have always deeply valued privacy, for it has been said that, "[o]ur personhood must remain inviolate: that is what privacy protects; that is its principle."[98] The importance placed on privacy creates tension in a world that now encourages the exposure of an online identity. If individuals do not undertake careful planning during life to

---

[94] Walker, *supra* note 2 at 70; RESTATEMENT (SECOND) OF TRUSTS § 147 cmt. a (AM. LAW INST. 1959).

[95] Walker, *supra* note 2, at 70.

[96] *Id.* at 71.

[97] *Id.*

[98] Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 739 (1989).

grant lawful consent to fiduciaries to access digital assets after death, accounts such as social media, email, and cryptocurrency could be lost forever. As state and federal laws prove to be inevitably slow in catching up to a technologically-advanced world full of digital assets, families and practitioners need to plan for digital death. In order to avoid complications, individuals must do their best to consult practitioners before they die, and practitioners must do their best to ensure that, if granted a decedent's consent, loved ones may access important digital assets after an individual's passing. Otherwise, privacy interests could prevent digital assets from ever being accessed, and along with their owners, these assets will suffer digital, but nevertheless permanent, death.