Digital Asset Planning, Password Sharing & the Risk of Liability

By: Carl M. Szabo & Jacklyn Kurin[1]

Overview

This whitepaper seeks to provide guidance to attorneys and the families they advise on legal methods for accessing a decedent's digital accounts and obtaining the contents therein. This paper explains why the alternative method proposed here is preferable to the current approach many have adopted—sharing passwords— which risks the possibility of civil liability and even criminal punishment. And because of that and other drawbacks, this paper recommends that fiduciaries,[2] whether they be trust and estate attorneys or family members, should instead use services like Directive Communication Systems, Inc. (DCS), which provide a lawful, effective, and secure means for obtaining a decedent's digital assets.

Digital Asset Planning Is Essential

The likelihood of working with a client who has some type of digital asset is practically certain. Since 2005, the percentage of American adults who have a social media account has increased from 5% to 69%.[3] On average, internet users have 7 social media accounts (up from 3 in 2012).[4] And that's number doesn't include other digital assets individuals may accumulate in their

---

[1] Carl M. Szabo is Senior Policy Counsel and Jacklyn Kurin is Law Clerk for NetChoice

[2] A fiduciary is a person with the legal authority to manage another's property and the duty to act in that person's best interests.

[3] *Social Media Fact Sheet*, PEW RESEARCH CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/social-media/ ("When Pew Research Center began tracking social media adoption in 2005, just 5% of American adults used at least one of these platforms. By 2011 that share had risen to half of all Americans, and today 69% of the public uses some type of social media.").

[4] Jason Mander, *Internet users have average of 7 social accounts*, GLOBAL WEB INDEX (Jun. 9, 2016), http://blog.globalwebindex.net/chart-of-the-day/internet-users-have-average-of-7-social-accounts/

lifetime: emails, bitcoins, domain names, photos, etc.[5] Naomi Cahn, a George Washington University professor, estimates the average person has more than 25 different accounts and passwords.[6] Back in 2011, McAfee found that the average American's digital assets were worth $55,000—an amount that is guaranteed to increase.[7] Gerry Beyer, a Texas Tech University School of Law professor, predicts that the amount and types of digital assets will only grow; thus, they will become extremely important to the next generation in their digital planning. Beyer says, "As people invest more information about their activities, health, and collective experiences into digital media, the legacies of digital lives grow increasingly important."[8]

But because online service policies are as different as snowflakes, each having a different policy for obtaining digital assets,[9] attorneys and heirs face an increasing burdensome, time consuming, and emotionally straining endeavor in obtaining what could be highly sentimental effects or important financial assets. Many states, including those that have adopted a version of UFADAA[10] or RUFADAA,[11] have laws that are woefully inadequate in addressing digital asset

---

[5] Digital assets consist of a person's digital property and electronic communications." Digital assets can be software (Word, Excel, Turbo Tax, Quicken); stored information on a hard drive, backup drive, CD, DVD, or thumb drive; on-line presences such as web sites, blogs, and social media accounts; online email, bank, brokerage, financial, shopping, and travel accounts; and on-line gaming pieces, photos, digital music, client lists, bitcoins, and even digital art." Victoria Blachly, *Uniform Fiduciary Access to Digital Assets Act: What UFADAA Know*, 29 PROB. & PROP. 4 (July/Aug. 2015), http://www.americanbar.org/publications/probate_property_magazine_2012/2015/july_august_2015/2015_aba_rpte_pp_v29_3_article_ blachly_uniform_fiduciary_access_to_digital_assets_act.html.

[6] Digital asset management: 4 steps for protecting your digital legacy, AMERIPRISE FINANCIAL, https://www.ameriprise.com/research-market-insights/financial-articles/insurance-estate-planning/protecting-your-digital-assets/.

[7] *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.

[8] Gerry W. Beyer, *Web Meets the Will: Estate Planning for Digital Assets*, 20 NAECP J. OF ESTATE & TAX PLANNING 28, 31 (First Quarter 2015), https://www.naepc.org/journal/issue20p.pdf. Beyer is the Governor Preston E. Smith Regents Professor of Law at Texas Tech University School of Law and contributor to NAELA and NAECP journals.

[9] Policies vary on what kind of digital assets heirs can obtain, the process for requesting them, and may use different criteria for who can make a request, what documentation is required to process request, evaluation of verification, standards for removing content, etc.

[10] The Uniform Fiduciary Access to Digital Assets Act (UFADAA) is model legislation that permits appointed fiduciaries to access digital assets as appropriate. If a person fails to plan, the same court appointed fiduciary that manages the person's tangible assets can manage the person's digital assets, distributing those assets to heirs or disposing of them as appropriate. Longstanding fiduciary law exists that allows a representative to stand in the shoes of a deceased or incapacitated person to recover real or tangible property. UFADAA was meant to clarify that those same laws apply to digital property. States that have enacted legislation based on UFADAA are Delaware (Del. Code tit. 12 § 5001 to 5007), Hawaii (Hawaii Rev. Stat. §§ 556A-1), Iowa (2017 S.B. 333), South Dakota (2017 H.B. 1080), and Utah 2017 H.B. 13).

[11] The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) is model legislation that extends the traditional power of a fiduciary to manage tangible property to include management of a person's digital assets. The act allows fiduciaries to manage digital property like computer files, web domains, and virtual currency, but restricts a fiduciary's access to electronic communications such as email, text messages, and social media accounts unless the original user consented in a will, trust, power of attorney, or other record. Several states have enacted legislation that is based on RUFADAA. These states are Arizona (Ariz. Rev. Stat. §§ 14-13101), Arkansas (2017 H.B. 2253, Act 886), California (Calif. Prob. Code §§ 870), Colorado (Colo. Rev. Stat. §§ 15-1-1501), Connecticut (Conn. Gen. Stat. § 45a-334b), Florida (Fla. Stat. §§ 740.001), Idaho (Idaho Code §§ 15-14-101), Illinois (755 ILCS 70/1), Indiana (Ind. Code Ann. § 32-39-1-1), Kansas (2017 S.B. 63), Maryland (Md. Estates & Trust Code §§ 15-601), Michigan (Mich. Comp. Laws §§ 700.1001), Minnesota (Minn. Stat. §§ 521A.01), Mississippi (2017 H.B. 849), Nebraska (Rev. Stat. Neb. §§ 30-501 to -518 -), New Mexico (2017 S.B. 60), North Carolina (N.C. Gen. Stat. §§ 36F-1), North Dakota (2017 H.B. 1214), Oregon (2016 S.B. 1554), South Carolina (S.C. Code Ann. §§ 62-2-1010), Tennessee (Tenn. Code §§ 35-8-101), Vermont (2017 H.B. 192, Act 13), Washington (Rev. Code Wash. §§ 11.120.010), Wisconsin (Wisc. Stat. § 711.01), and Wyoming (Wyo. Stat. § 2-3-1001).

issues. Often these laws fail to authorize fiduciaries to perform basic functions, like obtaining a decedent's emails and wall postings. Thus, even families who live in one of these states are not immune from this ordeal and may find themselves at the mercy of the online service's discretion.

"As people invest more information about their activities, health, and collective experiences into digital media, the legacies of digital lives grow increasingly important."

Faced with this daunting task, numerous attorneys have adopted a well-intentioned, but misguided approach of telling clients to share their passwords with their spouses or likely heirs. By doings so, attorneys are potentially breaking the law. Furthermore, their recommendations to clients to keep their passwords and account information in a safe location or take other precautionary measures are unlikely to save their clients or themselves from federal or state prosecution.

The Computer Fraud and Abuse Act

Each state and Congress has enacted a Computer Fraud and Abuse Act (CFAA) that criminalizes (or at least, creates civil liability for) the unauthorized access of computer hardware and devices and the data stored thereon. The federal CFAA provides:

> (a) Whoever— . . . (2) *intentionally accesses* a computer *without authorization* or *exceeds authorized access*, and thereby obtains— . . . (C) information from any protected computer if the conduct involved an interstate or foreign communication; . . . shall be punished as provided in subsection (c) of this section.[12]

Courts have interpreted that "access" refers to whether the owner of the computer or online service granted the defendant permission use it.[13] Unfortunately, in absence of the system owner's permission, the fact that a decedent user "authorized" a fiduciary to stand in his place, either through his will or by a state's default digital asset law, might not be enough to bar prosecution under the CFAA.

Most online services[14] require the user of an account (1) to enter a password to access the service and (2) to agree to abide by the terms of service agreement (TOSA often includes several agreements such as a terms of service or use and a privacy policy). An online service permits an individual to access and use the online service because he has agreed to abide by the TOSA, which identifies permissible and prohibited conduct. Almost all online services prohibit users

---

[12] 18 U.S.C. § 1030(a)(2)(C).

[13] *See, e.g.*, 18 U.S.C. §§ 2701 and 1030.

[14] Online services that store digital assets on their servers are called "custodians." The TOSA usually governs the terms by which an individual can obtain the user's digital assets from the custodian.

from sharing their passwords or at least strongly discourage the behavior. Thus, by accessing another's digital accounts or assets, the fiduciary may be violating the online service's TOSA and, in turn, the federal CFAA.

Some federal prosecutors have used the CFAA to prosecute defendants based solely on violations of a website's TOSA. In 2006, prosecutors convicted a mother under the CFAA for violating MySpace's TOSA by creating a fake "MySpace" profile to bully a child who then committed suicide.[15] Ultimately, the trial judge overturned the mother's conviction because the government's statutory interpretation was constitutionally vague.[16] In 2013, prosecutors pursued multiple CFAA charges against Aaron Swartz, a Harvard fellow and computer programmer, for downloading, without permission, 4.8 million academic articles from the JSTOR digital library system, through MIT servers.[17] Facing the possibility of 50 years in prison, Swartz tragically took his life. [18]

Despite these outcomes, the DOJ intends to continue to prosecute TOSA violations, as evidenced by this testimony excerpt by Richard W. Downing, who at the time was deputy chief of the DOJ's Computer Crime and Intellectual Property Section Criminal Division:[19]

> Finally, on behalf of the Department I want to address concerns regarding the scope of the CFAA in the context of the definition of "exceeds authorized access." In short, the statute permits the government to charge a person with violating the CFAA when that person has exceeded his access by violating the access rules put in place by the computer owner and then commits fraud or obtains information. *Some have argued that this can lead to prosecutions based upon "mere" violations of website terms of service or use policies.* As a result, some have argued that the definition of "exceeds authorized access" in the CFAA should be restricted to disallow prosecutions based upon a violation of contractual agreements with an employer or service provider. *We appreciate this view, but we are concerned that restricting the statute in this way would make it difficult or impossible to deter and address serious insider threats through prosecution.*[20]

---

[15] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[16] *Id.* at 464.

[17] United States v. Swartz, 1:11-cr-10260, 106 (D. Mass. filed Jan. 14, 2013).

[18] *See* Andrea Peterson, *The Law Used to Prosecute Aaron Swartz Remains Unchanged a Year After His Death*, WASH. POST (Jan. 11, 2014), http://tinyurl.com/otpk3d2.

[19] Downing currently serves as Deputy Assistant Attorney General (Acting) in DOJ's Computer Crime and Intellectual Property Section Criminal Division.

[20] Richard W. Downing, *Cybersecurity: Protecting America's New Frontier*, Committee on Judiciary (Nov. 15, 2011) (emphasis added), http://tinyurl.com/k2nv3o3 (testimony before the House Judiciary Committee Subcommittee on Crime, Terrorism, and National Security, presented on November 15, 2011).

Circuit Courts Have Held Non-Compliance with TOSA Violates CFAA

The CFAA criminalizes (and creates a private right of action against) a person who accesses a computer or online service *"*without authorization" or *"*exceeds authorized access."[21] Many circuit courts have held that violating a company policy, including a website TOSA, is sufficient grounds to constitute a criminal act under the CFAA.[22] Some circuit courts have interpreted that a person "exceeds authorized access" by breaching a private company policy. The 11th Circuit held that an employee who violates employer use restrictions "exceeds authorized access."[23] Similarly, the 1st Circuit held that former employees who violated confidentiality agreements by scraping data from their former employer's website, which was not within the website's authorized use, "exceeded authorized access."[24] The Ninth Circuit in *Nosal II* (2-1 majority) interpreted the CFAA's "without authorization" prong, applied to a former employee's use of another's password to access his former employer's databases to obtain proprietary information. Under the majority's standard, "a person necessarily accesses a computer account 'without authorization' if he does so without the permission of the system owner."[25]

Recently, in *Facebook, Inc. v. Power Ventures, Inc.,* a civil application of CFAA, the Ninth Circuit ruled that "a defendant can run afoul of the CFAA [under the "without authorization" prong] when he or she has no permission to access a computer or when such permission has been revoked explicitly."[26] The "no permission to access" language could potentially be viewed to extend to those who obtain access to an online account by using the account holder's password. Ultimately, courts have interpreted the CFAA applies to violations of TOSA and unauthorized use of passwords.

Many circuit courts have held that violating a company policy, including a website TOSA, is sufficient grounds to constitute a criminal act under the CFAA.

Liability Under Other Computer Laws

Password sharing may violate other federal and state laws. The Electronic Communications Privacy Act (ECPA) is a federal law that establishes standards for access to private information

---

[21] 18 U.S.C. § 1030(a)(2)(C).

[22] Several circuit courts have held that using a computer or computer system in a manner that fails to comply with a company policy, by itself, is insufficient for violating the CFAA. Nevertheless, because the vagueness of the CFAA statute and imprecise crafted legal standards, even these courts have upheld convictions for password sharing, *see United States v. Nosal,* 844 F.3d 1024 (9th Cir.2016) (*Nosal II*), and accessing an online service without permission, s*ee* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1066 (9th Cir.2016). For example, the majority in *Nosal II* denied it was outlawing password sharing, but the legal standard the court crafted achieves the opposite result. *Nosal,* 844 F.3d 1024.

[23] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

[24] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-84 (1st Cir. 2001).

[25] *Nosal,* 844 F.3d at 1055 n.4 (Reinhardt, J., dissent) ("The term 'system owner' refers to the central authority governing user accounts, whether the owner of a single computer with one or several user accounts, a workplace network with dozens, or a social networking site, bank website, or the like, with millions of user accounts.").

[26] *Power Ventures, Inc.*, 844 F.3d at 1066.

transmitted and stored on the internet, such as emails, photos, or direct messages. The Stored Communications Act (SCA), a component of (ECPA), has two pertinent sections that impact a fiduciary's and heir's ability to access or obtain a decedent's electronic communications.

Section 2701 provides criminal penalties for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided or … intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . . ." [27] Courts have interpreted that "without authorization" and "exceeds authorized access" in the SCA have the same meaning as they do under the CFAA.

Under Section 2702, an online service that stores or maintains electronic communications risks civil liability if it divulges a user's emails or the contents of other communications without the user's "lawful consent." [28] The SCA permits the online service to disclose the user's communications if the service has the lawful consent of the "originator or an addressee or intended recipient of such communication,"[29] but even then, disclosure isn't mandatory and the online service can refuse an heir's request.[30] This deference to the online service's discretion is exemplified by *In re Facebook*, where the Northern District Court of California held that the SCA did not compel Facebook to give a deceased user's information to her family. The court stated that "under the plain language of Section 2702, while consent may permit production by a provider, it may not require such a production."[31]

All fifty states have a computer fraud and abuse law.[32] The threshold for violating state law is lower than the federal CFAA. Therefore, defendants have been found to have violated the state

---

[27] 18 U.S.C. § 2701.

[28] 18 U.S.C. § 2702.

[29] *Id.*

[30] *Id.*

[31] In re Facebook, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012).

[32] Ala. Code §§ 13A-8-112, 13A-8-113 (computer trespass); Alaska Stat. § 11.46.740 (computer trespass); Ariz. Rev. Stat. Ann. § 13-2316 (crime of computer tampering); Ark. Code Ann. §§ 5-41-101 to -206 (computer trespass); Cal. Penal Code § 502 (computer trespass); Colo. Rev. Stat. Ann. § 18-5.5-101 to -102 (computer trespass); Conn. Gen. Stat. Ann. §§ 53a-250 to 53a-261 (computer trespass); Del. Code Ann. tit. 11, §§ 931 to 941 (computer trespass); Ga. Code Ann. § 16-9-93(c) (the crime of computer invasion of privacy exists when a person uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person); Ga. Code Ann. §§ 16-9-90 to 16-9-94 (computer trespass); Haw. Rev. Stat. §§ 708-890 to 708-895.7 (computer trespass); Idaho Code §§ 18-2201, 18-2202 (computer trespass); 720 Ill. Comp. Stat. 5/16D-3 (crime computer tampering); 720 Ill. Comp. Stat. Ann. 5/17-50 to -55 (computer fraud and access); Ind. Code Ann. § 35-43-1-4 (crime of computer tampering); Iowa Code § 716.6B (computer trespass); Kan. Stat. Ann. § 21-5839 (computer trespass); Ky. Rev. Stat. §§ 434.840, 434.845, 434.850, 434.851, 434.853, 434.855, 434.860 (computer trespass); La. Rev. Stat. Ann. § 14:73.7 (crime of computer tampering); Me Rev. St. Ann. tit. 17-A, § 432 (criminal invasion of computer privacy); Md. Code Ann., Crim. Law § 7-302 (computer trespass); Mass. Gen. Laws Ann. ch. 266, § 33A (computer trespass); Mich. Comp. Laws §§ 752.791 to 752.797 (computer trespass); Minn. Stat. Ann. §§ 609.87 to 609.893 (computer trespass); Mo. Rev. Stat. § 537.525 (civil remedy); Miss. Code Ann. § 97-45-7 (crime of computer tampering); Mo. Ann. Stat. § 569.095 (crime of computer data tampering); Mo. Ann. Stat. § 569.099 (crime of tampering with computer users); Mont. Code Ann. §§ 45-2-101, 45-6-310, 45-6-311 (computer trespass); Neb. Rev. Stat. §§ 28-1341 to 28-1348 (computer trespass); Nev. Rev. Stat. §§ 205.473 to 205.513 (computer trespass); N.H. Rev. Stat. Ann. §§ 638:16 to 638:19 (computer trespass); N.J. Stat. Ann. §§ 2A:38A-1 to 2A:38A-6 (computer trespass); N.M. Stat. Ann. §§ 30-45-1 to 30-45-7 (computer trespass); N.Y. Penal Law §§ 156.20, 156.25, 156.26, and 156.27 (crime of computer tampering); N.C. Gen. Stat.

computer fraud law even if he is not guilty of a federal CFAA crime.[33] In some instances, password sharing also violates state trade secret laws.[34]

Trust and Estate Attorneys Fear Criminal Prosecution for CFAA & SCA Violations

Fiduciaries are bound to preserve the assets of the estates they manage. But they face a Catch-22 as they "risk civil liability if they refuse to manage a decedent's digital assets or criminal and civil liability if they perform their duties."[35] Prominent trust and estate experts and law associations[36] recognize the CFAA and SCA pose a credible and significant threat to them and their clients. In 2015, the President of the American College of Trust and Estate Counsel (ACTEC) pleaded with Senator Flake and Representative Issa to revise the SCA and CFAA "to clarify that fiduciaries are authorized to administer a person's digital assets" because under the current language, fiduciaries, by performing their legally obligated duties, risk "violating federal privacy laws or criminal laws."[37] Unfortunately, all reform efforts have been unsuccessful; as such, the threat of criminal prosecution and civil liability remains.

These fears of prosecution are more likely to be realized in light of the *Nosal II* decision, where the Ninth Circuit upheld the defendant's CFAA conviction even though he didn't use the password and only instructed former employee to use it. Consequently, attorneys might be

---

Ann. §§ 14-453 to 14-458 (computer trespass); N.D. Cent. Code § 12.1-06.1-08 (computer trespass); Ohio Rev. Code Ann. §§ 2909.01, 2909.04, 2909.07(A)(6), 2913.01 to 2913.04 (computer trespass); Okla. Stat. Ann. tit. 21, §§ 1951 to 1959 (computer trespass); Or. Rev. Stat. Ann. § 164.377 (computer trespass); 18 Pa. Cons. Stat. Ann. § 5741 (computer trespass); R. I. Gen. Laws § 11-52-8 (crime of tampering with computer source documents); S.C. Code Ann. §§ 16-16-10 to 16-16-40 (computer trespass); S.D. Codified Laws §§ 43-43B-1 to 43-43B-8 (computer trespass); Tenn. Code. Ann. § 39-14-602 (crime of computer tampering); Tex. Penal Code § 33.02 (computer trespass); Utah Code §§ 76-6-702 to 76-6-705 (computer trespass); Vt. Stat. Ann. tit. 13, §§ 4101 to 4107 (computer trespass); Va. St. Ann. § 18.2-152.5 ("A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person"); Wash. Rev. Code Ann. § 9A.52.110-130 (computer trespass); W. Va. Code § 61-3C-12 (crime of computer invasion of privacy occurs when a person uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person); Wis. Stat. Ann. § 943.70 (computer trespass); Wyo. Stat. Ann. §§ 6-3-501 to 6-3-506, 40-25-101 (computer trespass).

[33] *See, e.g.*, DocMagic, Inc. v. Ellie Mae, Inc., 745 F. Supp. 2d 1119 (N.D. Cal. 2010) ("California Comprehensive Computer Data Access and Fraud Act ("CCDAFA"), Cal.Penal Code § 502 . . . is similar to the CFAA, but prohibits a wider range of conduct. See Cal.Penal Code § 502(c)(1)-(9)."); Capitol Audio Access, Inc. v. Umemoto, 980 F. Supp. 2d 1154, 1159–60 (E.D. Cal. 2013) (dismissing the CFAA claim but finding liability under CCDAFA).

[34] *See, e.g.*, Umemoto, 980 F. Supp. 2d 1154 ("Online news publisher's allegations that a subscriber used a password intended for individual access to publisher's website to share publisher's content with over 100 people, in violation of publisher's user license agreement, and allegations that the sharing allowed those people to obtain economic value, stated a claim for violation of California's adoption of the Uniform Trade Secret Act (CUTSA), Cal.Civ.Code § 3426.1(b), (d)(1).").

[35] Sasha A. Klein & Mark R. Parthemer, *Who Will Delete You? Understanding Fiduciary Access to Digital Assets*, 30 PROB. & PROP. 4 (July/Aug. 2016).

[36] American Bar Association, National Academy of Elder Law Attorneys, National Association of Estate Planners & Councils, and American College of Trust & Estate Counsel.

[37] Letter from ACTEC President Kathleen R. Sherby to Sen. Jeff Flake and Rep. Darrell Issa (Jan. 28, 2015), http://www.actec.org/assets/1/6/ACTEC-Proposed-revisions-to-the-ECPA-and-to-the-CFAA-1-28-2015.pdf ("For example, the personal representative appointed to administer a deceased person's estate should be able to access the decedent's digital assets, including the contents of the deceased person's electronic communications, to carry out his or her fiduciary duties in administering the deceased person's estate without violating federal privacy laws or criminal laws.").

charged with conspiracy to violate CFAA for simply advising their clients to share their passwords without the online service's approval.

Fiduciaries face a Catch-22 as they "risk civil liability if they refuse to manage a decedent's digital assets or criminal and civil liability if they perform their duties."[38]

Password Sharing is Ineffective

Aside from the illegality, password sharing is an ineffective and insecure method for obtaining a decedent's digital assets. Currently, many attorneys advise their clients to write down the information to access their online accounts (username, password, and answers to security questions) in an inventory document and put it in a secure place. This method is ineffective because users regularly change their passwords while using an online service, either involuntarily or because the online service requires it. Also, if the user fails to update that information, the inventory will be useless later in accessing his online accounts.

Password sharing cannot keep up with online services that are constantly updating their user policies and introducing new digital asset protocols. Even if a user named a fiduciary in his will, he still might designate a recipient of his digital assets through the online service's user choice tool. If the user designates someone other than the fiduciary, the fiduciary might be unable to access or obtain digital assets from the user's account. For example, consider Facebook's Legacy Contact tool. The user's widow would not be able to manage the user's Facebook Memorial Page if the user designated someone else as his Legacy Contact.[39] Even if the widow presents Facebook with a court order, Facebook may deny the widow's request to download content from her deceased husband's Facebook account.[40]

Password sharing also does not protect against human error. It doesn't prevent a fiduciary from accidentally deleting a decedent's account that held information required for settling the estate. Many popular online services warn users that once data is deleted, it is lost permanently. Families can also find themselves locked out of a decedent's account by failing to satisfy the online service's verification process. For example, Microsoft will permanently deny heirs access after three unsuccessful verification attempts.

Password Sharing is Insecure

A decedent's unmonitored or inaccessible online accounts are vulnerable to criminals who may seek to "hack these accounts, open new credit cards, apply for jobs, and even obtain state

---

[38] Klein & Parthemer, *supra* , note 34.

[39] *What data can a legacy contact download from Facebook?*, FACEBOOK, https://www.facebook.com/help/408044339354739?helpref=related (last visited Jun. 28, 2017); *What is a legacy contact on Facebook?*, FACEBOOK, https://www.facebook.com/help/1568013990080948 (last visited Jun. 28, 2017).

[40] *How do I request content from the Facebook account of a deceased person?*, FACEBOOK,

https://www.facebook.com/help/123355624495297?helpref=related (last visited Jun. 28, 2017).

identification cards."[41] The Bureau of Justice Statistics reported that 16.6 million American adults were victim of identity theft in 2012.[42] "[M]ore than half of adults who use social networks post information that puts them at risk for identity theft and other cybercrimes."[43] Thus, it is critical that a fiduciary can immediately monitor, protect, and secure the assets in a decedent's online accounts.

It is universally acknowledged that an individual should never write down his passwords because if the document fell into the wrong hands, then the individual would be exposed to identity theft and a parade of horribles. A criminal having your passwords and account information is worse than giving him keys to your house, because with your passwords he can access and drain your bank accounts, steal your premium membership gifts and rewards, use your subscription services, destroy priceless photos and documents, and commit other acts that have emotionally and financially devastating repercussions.

Alarmingly, as Beyer reports, clients giving family members their passwords while they're alive and well also can backfire. "For example, if a client gives his . . . daughter the online banking information to pay the client's bills while he . . . is sick, siblings may accuse her of misusing the funds. Further, a dishonest family member would be able to steal the client's money undetected."[44]

Solution to Digital Asset Management

Given the DOJ's zealotry in prosecuting TOSA violations as CFAA crimes, the growing number of federal courts applying the CFAA to breaches of company policies and their broadening the meaning of "access without authorization", and the increase of state computer laws that criminalize unauthorized password sharing, there is no benefit in continuing to advise clients to break the law. Moreover, attorneys risk violating their ethical obligations and breaching their fiduciary duties if they fail to disclose to their clients these potential pitfalls and liabilities associated with password sharing.

Considering these issues, both attorneys and clients need a lawful, effective, and secure solution for managing the client's digital assets. Companies like DCS provide the optimal solution. DCS, for example, provides a digital asset service that requires no account passwords, thereby avoiding any potential violation of federal or state CFAA laws. The no password requirement has the added benefit of minimizing ID theft and fraud potential. DCS also ensures the security of account data by using a system that meets PCI and HIPAA standards.

---

[41] *See* Beyer, *supra* note 5, at 40.

[42] Alexander Trowbridge, *Identity Theft Rises, Consumers Rage*, CBS NEWS (July 1, 2014), http://tinyurl.com/n72ycq3.

[43] Chelsea Ray, *'Til Death Do Us Part: A Proposal for Handling Digital Assets After Death*, 47 REAL PROP., TR. & EST. L.J. 3, 583, 588 (2013) (quoting Alex Pham, *Internet Security 101: What Not to Post on Facebook*, L.A. TIMES TECHNOLOGY (May 3, 2010), http://tinyurl.com/2f7crxy).

[44] *See* Beyer, *supra* note 5, at 33.

Online Services' Digital Asset Protocol		
Email	Password Policy	Digital Asset Protocol[45]
AOL	Don't share your password[46]	Delete/Deactivate/Access Account • Use deceased "master Username, Password and Account Security Question" to transfer ownership of the account for billing purposes[47] • Contact AOL Customer Service if you do not know User's information. • Third-party requester who is not listed under user's account or doesn't have an Aol account needs to AOL Customer Support Team Representatives at **1-800-827-6364**.

		Termination/Deactivation
		• AOL may terminate User's account after 90 days of inactivity
		• After termination, AOL may:
		  ○ delete User's data
		  ○ refuse to remove content or other information User posted
		  ○ refuse to reactivate User's account[48]

Google	Don't share your password[49]	Inactive Account Manager • User decides whether to share or delete his account after a set period of inactivity
		Access Account

[45] Online service's policies for deleting or accessing a decedent's account, and removing or downloading decedent's digital assets.

[46] *Protecting Your AOL Account*, AOL, https://help.aol.com/articles/protecting-your-aol-account ("Never disclose your password or Account Security Question (ASQ) to anyone. Don't send your password or ASQ in an email, Instant Message or chat room.").

[47] https://help.aol.com/articles/account-management-cancel-or-reactivate-your-aol-account

[48] *Terms of Service*, AOL (last updated Jun. 13, 2017), http://legal.aol.com/terms-of-service_full-terms/ "After we terminate or deactivate your account for inactivity or any other reason, we have no obligation to retain, store, or provide you with any data, information, e-mail, or other content that you uploaded, stored, transferred, sent, mailed, received, forwarded, posted or otherwise provide to us (collectively "posted" or "post") on the Services and may allow another user to register and use the username. We also have no obligation to remove any public data, content, or other information that you posted on a Service or to reactivate your account.").

[49] *Google Terms of Service*, GOOGLE (last updated Apr. 14, 2014), https://www.google.com/intl/en/policies/terms/ ("To protect your Google Account, keep your password confidential. You are responsible for the activity that happens on or through your Google Account.").

		• Designated representative must complete a two-part process
		  ○ Part 1: Submit required materials to Google, including information and documentation verifying Requester's identity, User's Gmail address and death certificate, etc.
		  ○ Part 2: Submit additional materials, including a court order
		• Processing time: several months
		• Google might deny request

Outlook[50]	Keep password confidential[51]	Delete Account & Download Content
		• Next of kin or designated representative provides info to custodian of records.
		  ○ Required documents: death certificate; proof requester is next of kin or designated representative; information about the User and his Outlook account.
		• Processing time: 48 hours
		• If verification fails, Outlook cannot tell requester which "information did not match." Only allows 3 attempts to pass verification.
		• Automatically deletes User's content and account after a period of inactivity
		  ○ content 1 year
		  ○ account 1 year and a month

		Delete/Deactivate Account • Only available to family members or designated representative
Yahoo!	Keep password confidential[52]	Delete Account • Designated representative can request User's account be closed and content permanently deleted after submitting required materials

[50] Same protocol applies to all other Microsoft services except for SkyDrive, MSN Dial-up, and Xbox Live.

[51] *Microsoft Services Agreement*, MICROSOFT (effective: Sept. 15, 2016), https://www.microsoft.com/en-US/servicesagreement/ ("To protect your account, keep your account details and password confidential. You are responsible for all activity that occurs under your Microsoft account or Skype account.").

[52] *Yahoo Terms of Service*, YAHOO (last updated Jun 13, 2017), https://policies.yahoo.com/us/en/yahoo/terms/utos/ ("You are responsible for maintaining the confidentiality of the password and account and are fully responsible for all activities that occur under your password or account. You agree to (a) immediately notify Yahoo of any unauthorized use of your password or account or any other breach of security, and (b) ensure that you exit from your account at the end of each session."); *Password Tips*, Yahoo, https://safety.yahoo.com/Security/STRONG-PASSWORD.html ("Your Yahoo ID and password are confidential information . . . . Do not write your password down. If you must write it down, keep it safe away in a place only you can access.").

		• Required documentation: A letter containing your request and stating the Yahoo ID of the deceased A copy of a document appointing the requesting party as the personal representative or executor of the estate of the deceased; A copy of the death certificate of the Yahoo account holder
		Download Content • Does not permit content download per TOSA
		Access Account • Does not permit others to log in to User's account per TOSA
Social Media	Password Policy	Digital Asset Protocol
Facebook	Explicitly prohibits password sharing[53]	Legacy Contact • User designates a person to manage his memorial page • User can allow Legacy Contact to download content in User's account

		Third-Party's Request for User's Content
		• Required documentation:
		  ○ Proof your family member or designated representative
		  ○ Court order
		• Facebook may still deny request

Pinterest	Keep your password secure[54]	Delete/Deactivate Account • Only available to family members or designated representative
		Not permit content download
Instagram	Keep your password secure[55]	Memorialization • Cannot edit memorial page or accept/deny friend requests • Does not permit content download • Does not permit others to log in to User's account
		Delete/Deactivate Account

[53] *Terms*, FACEBOOK (last updated Jan. 30, 2015), https://www.facebook.com/terms ("You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account . . . . You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.").

[54] *Terms of Service*, PINTEREST (Nov. 1, 2016), https://policy.pinterest.com/en/terms-of-service ("We ask that you keep your password secure. Please notify us immediately of any compromise or unauthorized use of your account.").

[55] *Terms of Use*, INSTAGRAM (effective: Jan. 19, 2013), https://help.instagram.com/478745558852511 ("You are responsible for keeping your password secret and secure.").

		• Only available to family members or designated representative
Twitter	Never give password to third-party	Delete Account
		Remove Content • Twitter may deny request based on public interest factors (e.g. Newsworthiness)
		Access User's Account • Not permit others to log in to User's account
Storage	Password Policy	Digital Asset Protocol
Dropbox	Don't share your password[56]	Access Account & Download Content • Requester must first complete a verification process. • Required documents: Court order[57] • Processing time: unknown[58] • Dropbox may deny request
Google Drive	Don't share password with anyone	See Google above
iCloud	Do not share your password[59]	Access & Download Content • Does not permit others to access or download content from iCloud
SpiderOak	Do not share your password[60]	Download Content • Does not release User's content • Need SpiderOak software and User's password to access and download content
Business	Password Policy	Digital Asset Protocol
Amazon	Keep your password confidential[61]	Access Account

[56] *Dropbox Terms of Service*, DROPBOX (effective: Feb. 10, 2017), https://www.dropbox.com/terms ("Safeguard your password to the Services, and keep your account information current. Don't share your account credentials or give others access to your account.").

[57] *Id.* ("establishing that it was the deceased person's intent that you have access to the files in their account after the person passed away, and that Dropbox is compelled by law to provide the deceased person's files to you").

[58] *Id.* ("process takes some time").

[59] *iCloud Terms & Conditions*, ICLOUD (last updated Mar. 1, 2017), https://www.apple.com/legal/internet-services/icloud/en/terms.html ("You further acknowledge and agree that the Service is designed and intended for personal use on an individual basis and you should not share your Account and/or password details with another individual.").

[60] *SpiderOak Privacy Policy*, SPIDEROAK (Jun. 2, 2016), https://spideroak.com/policy/privacy-policy ("You use SpiderOak at your own risk, and are responsible for taking reasonable measures to secure your account (such as choosing a strong, unique passphrase and keeping it secret).").

[61] *Conditions of Use*, AMAZON (last updated May 30, 2017), https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=508088 ("You are responsible for maintaining the confidentiality of your account and password and for restricting access to your account, and you agree to accept responsibility for all activities that occur under your account or password."); *Choose a Strong Password*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=10412241. ("it's important to change it periodically and keep your password private").

		• Seller Support can only communicate with a relative, spouse, or estate executor. • The account will need to be transferred to a new name and then closed or the new person can take legal responsibility for the account. • All items would be returned if closed within 30 days.[62]
Etsy	Keep your password secure[63]	Delete Account & Download Content • Must be designated representative or next of kin • Does not permit access to User's account • Required documentation: death certificate[64] • Might permit content download in rare instances
eBay	Don't share your password[65]	Delete/Access Account • Notify eBay of User's death • Required documentation: death certificate[66]
Entertainment	Password Policy	Digital Asset Protocol
Netflix	Do not share your password[67]	Deactivate Account • Need User's account name and password to deactivate account.
Google Play	Don't share your password[68]	*See* Google above
Amazon		Deactivate Account

[62] https://sellercentral.amazon.com/forums/message.jspa?messageID=3626420

[63] *Terms of Use*, ETSY (last updated Jun. 8, 2017), https://www.etsy.com/legal/terms-of-use/ ("Protect your password. As we mentioned above, you're solely responsible for any activity on your account, so it's important to keep your account password secure.").

[64] https://www.etsy.com/help/article/24695828180

[65] *Creating an eBay Password*, EBAY, http://pages.ebay.com/help/new/contextual/create_password.html ("After creating your password, protect it. Don't share your password with others.").

[66] http://community.ebay.com/t5/Buying-Selling-Basics/Removal-of-a-deceased-person-s-account/qaq-p/19018637; https://community.ebay.com/t5/Buying-Selling-Basics/What-happens-to-the-account-if-the-account-holder-dies-Can/qaq-p/21321332

[67] *Netflix Terms of Use*, NETFLIX (last updated Nov. 30, 2016), https://help.netflix.com/legal/termsofuse ("[T]he Account Owner should not reveal the password to anyone.").

[68] *Google Terms of Service*, GOOGLE (last updated Apr. 14, 2014), https://www.google.com/intl/en/policies/terms/ ("To protect your Google Account, keep your password confidential. You are responsible for the activity that happens on or through your Google Account.").

	Keep your password confidential[69]	• Need User's account name and password to deactivate account.[70]
		Transfer Content • Does not permit transfer of videos or Kindle books
iTunes	Don't share your password[71]	Transfer Content • Does not permit transfer of iTunes library
Hulu	Keep your password confidential[72]	Deactivate Account • Need User's account name and password to deactivate account
Financial	Password Policy	Digital Asset Protocol
PayPal	Prohibits password sharing[73]	Access Account & Obtain Balance • Requester must first complete a verification process. • Required documents: o A cover sheet from the executor (or a person who is duly appointed or authorized to administer the estate of the deceased customer) identifying the account by the primary email address, stating that the account holder is deceased and that the executor wishes to have the PayPal account closed. o A copy of the death certificate for the account holder. o A copy of a government issued photo ID (such as a driver's license, passport

[69] *Conditions of Use*, AMAZON (last updated May 30, 2017), https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=508088 ("You are responsible for maintaining the confidentiality of your account and password and for restricting access to your account, and you agree to accept responsibility for all activities that occur under your account or password."); *Choose a Strong Password*, AMAZON,https://www.amazon.com/gp/help/customer/display.html?nodeId=10412241. "it's important to change it periodically and keep your password private."

[70] https://www.amazon.com/forum/kindle?_encoding=UTF8&cdForum=Fx1D7SY3BVSESG&cdThread=Tx1962PFH4W513

[71] *Apple Media Services Terms & Conditions*, APPLE (last updated Sept. 13, 2016), https://www.apple.com/legal/internet-services/itunes/us/terms.html. "Your Apple ID is valuable, and you are responsible for maintaining its confidentiality and security."; *Security & Your Apple ID,* APPLE (Mar. 27, 2017), https://support.apple.com/en-us/HT201303. ("Never share your password or verification code with anyone else.").

[72] *Terms of Use*, HULU (May 3, 2017), https://www.hulu.com/terms ("Please keep your password confidential. You will not have to reveal it to any Hulu representative. Because you are responsible for all use of your account, including unauthorized use by any third party, please be very careful to guard the security of your password.").

[73] *User Agreement for PayPal Service*, PAYPAL (Apr. 27, 2017), https://www.paypal.com/gi/webapps/mpp/ua/useragreement-full ("[Do not] [r]eveal your Account password(s) to anyone else, nor may you use anyone else's password. We are not responsible for losses incurred by you including, without limitation, the use of your Account by any person other than you, arising as the result of misuse of passwords . . . . Not allow anyone else to have or use your Funding Source, password or PIN details . . . Never write your password or PIN in a way that can be understood by someone else . . . . Take care to make sure that no one sees your password or PIN when you use it."). .

		or state-issued ID) of the executor of the estate. ○ Legal documentation or a copy of the will that identifies the executor of the estate. • **Note**: If this PayPal account has a balance, we will also require a letter that specifies what to do with the money that remains in the account. • Once all necessary documentation has been received and reviewed, the account will be closed within 1-2 business days.[74]
Coinbase	**Keep your password secure**[75]	**Obtain Balance in Account** • Contact Coinbase to inform them of User's death • Required documentation: ○ Death Certificate ○ Last Will and Testament ○ Probate Documents (either Probate, Letters Testamentary, Letters of Administration, Affidavit for Collection or Small Estate Affidavit) ○ Current, valid government-issued photo identification of the person(s) named in the Letters Issued ○ A letter signed by the person(s) named in the Probate Documents instructing Coinbase on what to do with the balance of the Coinbase account.[76]

[74] https://www.paypal.com/us/selfhelp/article/How-do-I-close-the-PayPal-account-of-a-relative-FAQ1694

[75] *Coinbase User Agreement*, COINBASE (Jun. 22, 2017), https://www.coinbase.com/legal/user_agreement?locale=en-US ("You are responsible for maintaining adequate security and control of any and all IDs, passwords, hints, personal identification numbers (PINs), API keys or any other codes that you use to access the Coinbase Services.").

[76] https://support.coinbase.com/customer/en/portal/articles/2321225-how-do-i-gain-access-to-a-deceased-family-member-s-coinbase-account-