Bloomberg BNA

Tax Management Memorandum™

Digital Assets: Managing Fiduciary Access and Cybersecurity Risks for Client Information

By Holly Isdale[*]

At the risk of waxing nostalgic, the estate administration process used to be a lot easier. When someone died, the family and the executor had to inventory the assets, value them for tax purposes and then transfer the assets in accordance with the directives in the estate plan or appropriate laws. Finding assets was relatively easy; you could comb through the file cabinet and watch the mailbox for a forgotten bank account. Today, however, as we buy, sell, consume and communicate online, the only thing in our physical mailbox may be unwanted catalogs and junk mail. Correspondence of all forms has become virtual: records and receipts are stored online, maybe in email confirmations but more often, the information only exists in the online app of a retailer. An executor may not be able to access key information, or may not even know of its existence.

The challenge of managing digital assets is further complicated by the rate of change in technology and the social acceptance (and expectations) as to how that technology is used. It is not enough that the executor is grappling with a property interest governed by contracts that were not negotiated or designed with administration in mind, but the laws simply cannot keep pace with the rate of change, and shifting expectations on how technology will be used, to address this effectively. An executor must still exercise his fiduciary duty to collect and inventory all assets, manage and curate them, value them for tax purposes and transfer or otherwise dispose of the assets in accordance with the estate plan or appropriate laws. Now consider that the very asset may vanish if you are not attentive to how it is managed, curated, valued and transferred!

WHAT ARE DIGITAL ASSETS AND WHY DO WE CARE?

The Uniform Probate Code defines property to include ''both real and personal property or any interest therein and means anything that may be the subject of ownership.''[1] The executor is charged with collecting and managing all property interests, yet the very nature of these property interests is unclear in the digital arena.

In 2010, Eric Schmidt, CEO of Google, postulated that if all of the data created could be assembled — all information, all human knowledge, from the dawn of time to 2003 — it would amount to about five Exabyte of data (each Exabyte is a billion gigabytes). He then noted that, by 2010, the world was creating that same amount of content every two days — mostly in user-generated content such as photos, messages, social media posts, chats and blogs.[2] A nightmare for the executor to be sure!

Digital assets include the obvious items such as hardware (computers, tablets, cell phones), memory devices (thumb drives, CDs, floppy disks, etc.), software programs and the content from these programs. Yet the nature of the asset itself is constantly evolving. Digital assets can also include the apps on your smartphone, as well as the content stored through the app in the ''cloud.'' The nature of a digital asset can depend on the medium by which it is accessed, stored or recreated,[3] creating another burden for the executor to preserve the manner in which the asset is stored

[*] Holly Isdale is the founder and CEO of Wealthaven, LLC, a consulting firm focusing on governance issues affecting closely held family businesses and the creation and incubation of family offices. In her spare time, she publishes and speaks on digital assets (www.digitaldeath.com), as she is fascinated by the interplay of technology and law in all its aspects.

[1] Unif. Probate Code §1-201 (38) (as amended 2010).

[2] http://techcrunch.com/2010/08/04/schmidt-data/.

[3] As a quick example, consider the difference between playing

and how it may be accessed.[4] For some data, the information attached to the digital asset can have independent significance, requiring a different preservation method.[5]

Today, the average household has six or more Internet-connected devices, upwards of 15 or more in wealthier homes. Smartphones are owned by over 80% of Americans between 18-49 years of age.[6] Over 91% of Americans use cell phones of some sort, many of whom (34%) use it as their primary access to the Internet, forsaking desktop computers (which are seeming to become archaic, as ownership reached its peak in 2010 with 88%, declining now to 78% of adults under 30).[7] It is now possible to open a bank or investment account, fund it and trade online without ever receiving a paper notification or having to send in a physical signature.

The average Internet user, in addition to multiple email accounts, also has social media accounts, instant messaging, messages or communications within social media accounts. Online music storage has expanded beyond purchased songs on iTunes (which are non-transferable) to include curated playlists on multiple platforms; here the user may not have purchased any of the underlying music yet the playlist itself can have value. Photos may be stored online, but a new asset is created whenever these photos are edited or shared on different social media platforms such as Instagram, Snapchat, Pinterest or perhaps Facebook. At a minimum, posting the same photo across each platform brings into play multiple terms of service (TOS) contracts that must be reviewed to determine the ability of an executor or fiduciary to access each application.

While most of the content on our various digital devices may not have huge monetary value, it is important for the fiduciary to understand the extent of the content, and whether it has commercial or personal value, and then to preserve that accordingly.

GAINING ACCESS

The digital age has ushered in new definitions and expectations of privacy, with some unanticipated downsides as cybercrimes begin to proliferate. Privacy is no longer a ''condition'' of American life and is, instead ''a commodity to be purchased.''[8] While we readily share our email addresses, Twitter and other social media user names, our employment information, and photos, many times this information can be shared without our consent. Even benign sharing of photos, birthdates and travel plans can lead to unwanted attention and increase the risk of identity theft and fraud. Americans are increasingly concerned about the ability of organizations, both public and private, to protect personal information collected, despite stringent enforcement by governmental agencies of privacy policies.[9] Over half of Internet users surveyed were worried about information available about them online and only 9% felt they had controlled their online presence to any level of security. Privacy and control over our information is deeply rooted in American society; this has extended to include a right to control one's identity and information. Yet once data is online, it becomes difficult to control it. While Americans may recognize that they are unable to be ''untracked,'' they do want a voice in how personal information is used. A Pew Research survey showed 74% of Americans felt it was ''very important'' to be in control of who receives information and to control what information is collected about them, with 86% of respondents having taken steps to remove or mask their digital footprints.[10] Indeed, one of the most closely watched privacy cases in the courts recently was the battle between the FBI and Apple over access to an iPhone used by one of the terrorists in the San Bernardino shootings in late 2015.[11]

While fiduciaries and executors can cite bona fide reasons for needing access, most of the existing state and federal laws are focused on preserving the privacy of the user. There are three major laws that are cited when service providers are asked to divulge information about their users or their users' activities. The Computer Fraud and Abuse Act (CFAA)[12] was added in 1986 and criminalizes the intentional access of a computer without authorization (or where the

---

Pac-man on a mobile app vs. the original arcade game where you used a joystick. The experience of the game can be as important as the game itself.

[4] Pick Your Poison: The Types of Digital Assets and Digital Accounts; Storm Tropea, *Social Media Is Permanent, You Are Not: Evaluating the Digital Property Dilemma in Florida Probate*, 39 Nova L. Rev. 91, 97 (2014).

[5] In particular, information proving when a file was created, amended or otherwise altered can be important to preserve. For example, the value of certain types of digital art can hinge on whether there is adequate proof that no subsequent alterations occurred after the artist's death.

[6] http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

[7] http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

[8] http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

[9] www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert—Appendix—-4.15.14.pdf; https://www.sec.gov/investment/im-guidance-2015-02.pdf.

[10] http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/

[11] http://www.politico.com/story/2016/03/feds-move-to-cancel-iphone-hearing-221062.

[12] 18 U.S.C. §1030.

ISSN 0148-8295

user exceeds their authorization) and where the individual wrongfully obtains information from any protected computer. A 1994 amendment allowed for civil actions to be brought under the statute as well. While the definition of ''protected computer'' is defined as one owned or used by a government or financial institution, the scope of the law applies to any computer used in interstate or foreign commerce or communication, essentially opening its application to any internet-connected device in today's Internet of Things (IoT).

In addition to suits brought under the CFAA, service providers are also governed by privacy restrictions in the 1986 Electronic Communications Privacy Act (ECPA),[13] which was enacted as an update of the Federal Wiretap Act of 1968 and extended the protection of communications to computers and other digital and electronic communications. Subsequent legislation, including the USA PATRIOT Act, has clarified and updated the ECPA to keep pace with the changing technology while balancing the need for greater governmental surveillance to fight terrorism. In general, the ECPA, as amended, protects privacy interests in all wire, oral and electronic communication while those communications are being made, are in transit and when they are stored electronically, on computers or into their digital forms.

While the ECPA accords certain types of communications more privacy and legal protection than others, it still prevents a service provider from disclosing information voluntarily. The Act permits disclosure of some items upon receipt of a subpoena, while other information may only be divulged through a special court order or a search warrant.

The ECPA also incorporates the Stored Communications Act (SCA),[14] which is at the heart of the FBI/Apple dispute and haunts many executors and fiduciaries as well in their attempts to access information. The SCA prohibits public providers of electronic communication services (ECS) as well as remote computing services (RCS) from ''knowingly divulge[ing] to any person or entity the contents of a communication which is carried or maintained on that service'' as well as information pertaining to the subscriber or customer of the service. An ECS is ''any service which provides to users. . . the ability to send or receive wire or electronic communications,''[15] while a RCS means the ''provision to the public of computer storage or processing services by means of an electronic communications system.''[16] To put into context, in *Crispin v. Christian Audigier, Inc.*, Facebook was considered to have acted as an ECS for purposes of the private messaging function, providing an ability to send or receive wire or electronic communications, while at the same time acting as an ECS or RCS for purposes of user's wall postings and comments.[17] In *In re Search of Google Email Accounts*, the Government filed search warrants to obtain contents of six third-party e-mail accounts hosted by a web-based e-mail provider. The holding stated modification of the warrant requiring provider to provide the government with e-mail correspondence was warranted, and the provider's application to modify the warrant and the resulting order would be unsealed.[18]

The importance of being considered either an ECS or RCS (or both) is that the SCA prohibits either provider from knowingly sharing information about user accounts, even the existence of that account, as well as information stored on that account. So while your posts to Facebook might be open to the world, depending on your privacy settings, Facebook itself cannot share that you have an account or what is on it without violating the SCA. Violations of the SCA are considered criminal infractions, resulting in fine or imprisonment,[19] although civil liability can arise as well.

The SCA grants providers a right to disclose information ''with the *lawful consent* of the originator or an addressee or intended recipient of such communication, or the subscriber'' in the case of remote communication service providers.[20] Congress, however, failed to define the term ''lawful consent,'' creating a challenge for fiduciaries who seek to access information on these systems.[21] While a fiduciary can certainly claim that the nature of his role places him in the shoes of the decedent, most of the court cases have taken the position that, absent clear written authorization, the fiduciary does not have this ability to demand access to information.

In *In Re Facebook, Inc.*,[22] Sahar Daftary, a young successful model, died after falling from a balcony. Her parents asked Facebook to release her messages in hopes of finding out her state of mind at the time of

---

[13] 18 U.S.C. §2510–§2522.

[14] 18 U.S.C. §2701–§2712.

[15] 18 U.S.C. §2510(15).

[16] 18 U.S.C. §2711(2).

[17] 717 F. Supp. 2d 965, 980–82, 989–90 (C.D. Cal 2010).

[18] *In re Search of Google Email Accounts*, 99 F. Supp. 3d 992 (D. Alaska 2015). *See also Viacom Intern. Inc. v. Youtube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (''[SCA] §2702 contains no exception for disclosure of [private videos and the data which reveal their contents] pursuant to civil discovery requests.'').

[19] 18 U.S.C. §2701.

[20] 18 U.S.C. §2702(b)(3). Emphasis Added.

[21] 18 U.S.C. §2702(b).

[22] 923 F. Supp. 2d. 1204 (N.D. Cal 2012).

ISSN 0148-8295

her death. Daftary's mother, the executor under her daughter's will, asserted that she had a right to access the Facebook account but the court ruled in favor of Facebook, noting that the SCA prohibited the sharing of the information without the subscriber's permission. Another case involved the Yahoo email account of a Marine killed in Iraq, Justin Ellsworth, whose family successfully sued Yahoo to retrieve the contents of the email account of the deceased soldier. While the father/executor did not gain access to the account itself, he was able to obtain a download of the information. Yahoo subsequently changed their terms of service (TOS) contract following the Ellsworth suit to clarify that the account was non-transferable and that, upon receipt of a death certificate, the account would be terminated and contents deleted.[23]

Likewise, since the *Daftary* case and presumably upon receiving similar requests that did not reach the courts, Facebook has added a ''legacy contact'' feature whereby a user can designate someone to post to their timeline after their death. This feature once activated, shuts down much of the functionality of a Facebook page, making it an ''In Memoriam'' site. The legacy contact is not able to log in to Facebook as the user or access private messages. They can, however, update and archive photos and posts, usually posting news of the death and funeral information. (Indeed, there is a growing sociological interest in the rise of ''digital mourning'' as these social media pages can stay active for years with an estimated 30 million profiles on Facebook that have ''outlived'' their creators).[24]

Despite these steps, most service providers do not have procedures in place to allow for a transfer of the account or to authorize the sharing of information beyond the mere existence of an account. Digital service providers still face potential civil liabilities if they divulge information, even if a fiduciary is able to provide the consent and the provider voluntarily complies with the information request. In addition, the Federal Trade Commission (FTC) has actively pursued penalties against service providers who violate their privacy policies, albeit in non-digital estate administration situations.[25]

STATE LEVEL RESPONSES

A number of states have attempted to address the issue of digital assets and enacted legislation relating to the ability of executors and fiduciaries to access and control digital assets. The earliest statutes usually covered only email accounts or only addressed access by parents to a minor's email accounts.

UFADAA, PEAC AND NOW REVISED UFADAA

Recognizing a need for consistency across state laws, the Uniform Laws Commission began a project around fiduciary access, culminating in the approval in 2014 of the Uniform Fiduciary Access to Digital Assets (UFADAA) model act which provided that, if a fiduciary has access to tangible assets, they would also have the right to access digital assets. UFADAA attempted to remove many of the federal barriers to fiduciary access (and eliminate possible criminal penalties as well) by asserting that any fiduciary would be affirmatively authorized under the CFAA and SCA, thus protecting service providers from criminal or civil liability if they provide information on a user or his account. The model act was designed to apply only where the fiduciary, conservator, agent or personal representative had received affirmative, written authorization to access the data under the terms of the relevant documentation (power of attorney, will, revocable trust, etc.).

In particular, UFADAA was designed to ensure that a fiduciary with authority over digital property would have the ''same authority as the account holder(s)'' and be considered to have the ''lawful consent of the account holder(s),'' thus would be considered ''authorized user(s) of the account(s).'' Similar authority is given to agents, conservators, personal representatives and trustees under the model legislation, albeit with some differences in how this authority would be triggered. For example, an agent or conservator must be specifically given authority over the protected person's or agent's digital property, a trustee must be granted such authority under the terms of a trust, but a personal representative (or executor) is implicitly authorized by virtue of their role.

Delaware adopted a version of UFADAA in 2014.[26] While the model UFADAA required affirmative action by a decedent, the Delaware statute presumed consent unless a decedent revoked it. Several other state legislatures took up legislative initiatives to enact a version of UFADAA in 2014, but these efforts stalled due to opposition from service providers citing concerns over privacy and contract rights of all users. The service providers had been active in voicing their opposition during the Uniform Law Commission proceedings and shifted their lobbying efforts to the state leg-

[23] Order to Produce Information, *In re Estate of Ellsworth*, No. 2005-296, 651-DE (Mich. Prob. Ct. Mar. 4, 2005).

[24] http://www.huffingtonpost.com/2012/12/07/death-facebook-dead-profiles_n_2245397.html.

[25] *In re Twitter, Inc.*, File No. 0923093 (FTC agreement containing consent order entered June 24, 2010). *See* 3 E-Commerce and Internet Law 27.06 (2015 update).

[26] 12 Del. C §5001 *et seq.*

ISSN 0148-8295

islatures, such that no other UFADAA-based laws were enacted. In addition to claiming that the laws went too far in granting unrestricted access, the service providers raised concerns around the privacy of other participants. Perhaps a decedent might be able to waive their own right to privacy and provide consent, but, they argued, the proposed model law did not sufficiently protect the interests of those with whom the decedent had communicated.

An alternative to UFADAA was proposed by NetChoice, the lobbying group representing many of the service providers. Called the Privacy Expectation Afterlife and Choices Act (PEAC),[27] this legislative proposal would require a probate court action to grant access, and only after the court is able to make certain findings of fact. PEAC also would direct the court to consider the user's actions in lifetime, including whether the user ever deleted records, posts or other contacts or made other elections as to the use of the assets. While this appears to contemplate an affirmative election by the user to allow for access (similar to the Facebook ''legacy contact''), it would also include the acceptance by the decedent of the applicable TOS contract provisions, perhaps eliminating any right to access by representatives.[28] Further, PEAC would affirmatively protect a provider from being compelled to disclose any records or contents of an account if there was any access to the account after the user's death. Studies sponsored by these lobbying groups showed overwhelming support for privacy of their digital communications.[29] While opponents raised concerns over the costs of a PEAC-based approach and the potential for inadvertent deletion or damage to digital assets from delays in the probate court, the PEAC approach did gain some momentum. Virginia enacted PEAC-based legislation in 2015.[30]

The ULC issued a revised version of UFADAA in July of 2015, amending many provisions to address privacy concerns around the 2014 version. The revised UFADAA allows a fiduciary to manage tangible property and includes digital assets such as computer files, web domains and virtual currencies (bitcoins) in this definition. The revised UFADAA does require affirmative consent to be given in a will, trust, power of attorney or other record to order to access electronic communications, such as email, text messages and social media accounts. The updated model legislation has now been enacted in four states (Florida, Wyoming, Oregon and Tennessee) and has been introduced in 22 other states.[31] It has received endorsements by Facebook and Google in addition to AARP and other advocacy groups.[32]

HOW TO PLAN IN UNCERTAINTY?

With the uncertainty around state laws, and the default approach in UFADAA now requiring clear authorization, it is important for advisors to incorporate authorization language in wills, revocable trusts and powers of attorney that addresses digital assets and the ability to access and manage these assets. The language should be broadly written to capture the changing nature of these assets and the decedent's intent to cover digital information and communications that may not exist at the time the authorization was created. At the same time, it is important to clearly provide the representative with the power to delete or destroy data, and to vest in them the ability to do so without repercussion. Not every estate warrants an archivist to sort through email communications and pictures posted on Facebook. However, it is important to understand what information might need to be preserved for posterity and what should be deleted. Given the technical nature of some of these accounts, many practitioners prefer to establish a separate digital executor or trustee, who can address these issues apart from the regular administrative actions of the trustee or executor.[33]

The concept of appointing a special executor just for digital assets can make sense when there are complex or unique assets, such as an active website or blog, significant online assets such as photos or social media accounts or if there are virtual currencies, such as bitcoins, that need to be handled and these skills are not suited to the normal executor. However, in these situations, practitioners should take care to specifically address the fiduciary liability of these special executors and how their actions will coexist with the actions of a broader executor function. Will actions by the special executor absolve the main executor of any liability or does that executor have a duty to oversee

---

[27] https://netchoice.org/library/privacy-expectation-afterlife-choices-act-peac/.

[28] This could open an interesting debate on the nature of the TOS acceptance. Unlike the other common form of Internet contract — known as ''click wrap'' agreements — browse wrap agreements do not require users to affirmatively click a button to confirm their assent to the agreement's terms; instead, a user's assent is inferred from his or her use of the website. *Long v. Provide Commerce, Inc.*, 245 Cal. App. 4th 855 (App. 2d Dist. 2016). Click wrap agreements 'have been routinely upheld by circuit and district courts.' *Sandler v. iStockphoto LP*, No. 215CV03659SVWJEM, BL 74276 at *3 (C.D. Cal. Feb. 5, 2016).

[29] https://netchoice.org/library/decedent-information/#poll.

[30] Va. Code §64.2-109 *et seq.*

[31] http://www.uniformlaws.org/Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets.

[32] http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20%282015%29.

[33] Sample language is available at www.digitaldeath.com.

ISSN 0148-8295

actions of the special executor? What right does the special executor have to use other resources of the estate to protect or manage the digital assets entrusted to his care?

Best practices would indicate that practitioners begin to insert specific digital language into all wills, revocable trusts and include clear authorization in powers of attorney as well. While some commentators (and commercial concerns targeting the digital asset space) will tout the benefits of broad stand-alone authorizations for digital access that can be downloaded and signed by anyone, it seems more prudent to link the authorization of digital access into a more conventional legal document where the appropriate state laws as to the revocation of such authorization would govern. Other benefits may arise from this approach as well. For example, the inclusion of an affirmative authorization to access digital assets in a revocable trust may offer additional flexibility in times of incapacity than under a power of attorney, perhaps allowing the trustee to argue that his or her use of passwords and accessing information as the user is not a violation of the TOS contract, a subtle but potentially important distinction.[34]

There has been some debate over the use of a stand-alone ''digital asset trusts'' to hold specific title to digital assets, and this may work for specific assets such as websites or virtual currencies. This approach, however, is unlikely to work in enough situations to warrant the effort of drafting it as part of a routine estate plan. In particular, the TOS contracts often prevent the transfer of social media or email accounts as well as other electronic content. It is worth mentioning that several commercial ventures have sprung up to address digital planning strategies, but some worry about the long-term viability of the company and the security of the information stored. In 2015, LastPass, one of the larger online ''Password vaults,'' was hacked[35] and the ''master passwords'' of users had to be updated, underscoring the risks of cybersecurity even in well-funded operations.

DON'T FORGET MEDICAL RECORDS

Apart from health care powers of attorney, few practitioners address access to medical documentation after death. With the rise of online medical records, virtual ''vaults'' for storage of files and the number of digital monitoring devices and apps, it is important to address access and control of this information as well. While digital asset authorizations might help to access apps or websites that a client has used and hopefully they have permissioned their executor to access online storage systems, few have included any guidance in their Health Insurance Portability and Accountability Act (HIPAA) documentation. All health care proxies or living wills should be adapted to include language clarifying the authority and access to medical and health information after death. The HIPAA statute clearly contemplates the post-mortem control of medical records; indeed, the 2013 changes to the statute reduced the privacy to 50 years post mortem, as opposed to the perpetual restrictions on this information in the original statute. Aside from some public policy exceptions, the person holding the HIPAA power, or the executor or personal representative, has ultimate authority to disclose or withhold medical information. For blended families, or same sex marriages where state-law conflicts may arise, it is important to clarify an intention to share medical information or health records. The surviving spouse may not need or care about this information but a biological child would benefit from knowing when and how a parent's health declined or when certain treatments were tried. For some families, ensuring access to a decedent's medical history might be the most enduring legacy they can provide, if it would allow for earlier detection and treatment of diseases in their descendants.

WHAT ARE THOSE TWEETS WORTH?

Once the executor or trustee has identified and accessed the assets, the question of ''value'' comes to the forefront. Most of us would agree that the value of our hardware devices is *de minimus* compared to the information that is contained on them or accessed through these devices. While sorting through endless emails or pictures of cats downloaded off of the Internet is not a great use of an executor's time, it's clearly important to know where valuable assets are held and what should be done with these assets. There are numerous stories of people finding cash in online accounts they forgot they had or recycling hard drives that contained important documentation, or Bitcoins, without checking the hard drive first.[36] Clearly business assets, such as domain names, websites, newsletters, blogs or other content, have a value and this

[34] *See* N.D. Cent Code Ann. §30.1-30-04. Power of attorney not revoked until notice. *Id.* Power of attorney not revoked until notice. *See* 20 Pa. Stat. and Cons. Stat. Ann. §5605 (West). Other powers of attorney not revoked until notice of death or disability. *See* Utah Code Ann. §75-5-502 (West). Health care power of attorney not revoked until notice. *See* Mont. Code Ann. §72-5-502 (West).

[35] https://blog.lastpass.com/2015/06/lastpass-security-notice.html/. *See also* http://www.forbes.com/sites/katevinton/2015/06/15/password-manager-lastpass-hacked-exposing-encrypted-master-passwords/#226ad20f5a66.

[36] http://www.nbcnews.com/news/other/it-worker-throws-out-hard-drive-loses-7-5-million-f2D11669738; https://www.cryptocoinsnews.com/thousands-bitcoins-lost-time/.

ISSN 0148-8295

value can change over time if not maintained. For these assets, the alternative valuation date might be appropriate but the executor or trustee will need to be aware of their own liability to understand and implement actions necessary to preserve the value of the assets during the administration period. Finally, even simple things, like travel pictures, can be monetized and the executor or fiduciary will benefit from releases in the relevant documents, exonerating them from having to find possible value in all assets.[37] Strong release language in the documents, providing relief to the executor and permitting them to abandon digital assets, or affirmatively delete assets, should be incorporated into any standard digital language templates.[38]

Finally, if transferable, the asset transfer must be done properly, which can require multiple steps depending on the asset. For many assets, the transfer is technically not permitted, but what liability accrues to the executor who transfers a Kindle, iPad or other device containing the decedent's electronic books and music?

WHAT'S THE RUSH?

For some clients, turning to the digital assets a month or so after a death may be sufficient, especially if the decedent was not very technologically savvy. Unfortunately, this may not be a wise delay, even if the executor believes that the situation is not pressing. Some email service providers will disable accounts after a relatively brief (60-day) period of dormancy. More importantly, the decedent's digital life may have been very connected to his or her financial one. Online magazines and subscriptions can automatically renew without anyone noticing, especially if these, like many online accounts with eBay, Etsy, Amazon, are connected to PayPal, which directly debits the bank accounts and, if the accounts run short, automatically rolls to credit cards (risking personal liability to the fiduciary or executor if they fail to control or protect the asset). Further, identity theft of decedents is on the rise, particularly because family and executors tend to take a few months to turn to the online accounts, giving thieves the opportunity to establish new credit cards, obtain identity papers and perhaps deplete bank or other accounts. Even for living individuals, a breach in one area can result in identify theft, often with catastrophic consequences, given flaws in how security practices vary across companies.[39] As such, it's better to err on the side of caution and establish control over the assets as soon as possible.

CYBERCRIME AND IDENTITY THEFT

It seems as though every day we are treated to another headline warning of larger and larger data breaches at large institutions. Spending on cybersecurity initiatives was $75 billion in 2015 and is expected to reach $170 billion by 2020.[40] Cybercrime has shifted from identity theft and fraud to target things like cars, home security systems, heating and cooling devices and medical devices — our Internet of Things has a downside and it is cybercrime.[41] While some may focus on the younger generation of ''digital natives'' that has never lived without email, the internet, social networks and mobile devices, fraud research shows that seniors lose up to $36.48 billion annually and almost 37% of seniors are affected by financial abuse in a five-year period. While a portion of this is allocable to ''normal'' fraud, such as abuse by caregivers, increasingly it is taking the form of identity theft and online scams (think Nigerian princes seeking your help!).[42] The FTC has noted that identity theft is one of its top complaints, often related to taxpayer ID theft and fraud. The ''mature market'' (denoted as age 50 or older!) is the single largest demographic of identity theft and fraud, with Florida, Georgia, California, Arizona and Texas having the highest incidence. Children aged 19 and under were the second largest demographic.[43] Cybercriminals, who go after capital or assets with monetary value, are now being joined by cyberspies, who steal information, such as passwords to accounts, and sell it on the black market as well as cyberactivists or ''hacktivists'' who hack into networks to disrupt them for political reasons but often sell the data they obtain on the black market where it can be used and stored for years.

What does this have to do with executors and fiduciaries you might ask? First and foremost, an executor and fiduciary has an affirmative duty of care to

---

[37] There are even companies forming to help monetize the value of online gaming assets, where picking up a special hat or sword in an online role playing game, can be worth several thousand dollars! Lest you think your teenage son is simply frittering his time away online — there is gold in those virtual worlds!

[38] See www.digitaldeath.com for sample language.

[39] http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.

[40] http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#3c69faf22191.

[41] http://www.csoonline.com/article/2984193/cyber-attacks-espionage/new-cybercrime-wave-drives-iot-security-spending.html.

[42] https://www.truelinkfinancial.com/news/latest-report-elder-financial-abuse-true-link-finds-36-48-billion-lost-annually-seniors/.

[43] http://amac.us/senior-id-theft-top-ftc-consumer-complaint/.

ISSN 0148-8295

protect the assets in their charge. As such, getting a credit report and filing for a lock on social security and other information has become an initial step in most estate administration processes. At the same time, law firms, banks, trust companies and other service providers are offering online access to client information, often posting copies of estate documents to these secure vaults. Some of the digital service providers are built around providing online repositories for the digital inventory that is provided. While not necessarily bad, there are a number of issues to be reviewed in any such offering, such as cybersecurity, access, preserving attorney-client privilege, etc.

Another concern may be whether federal laws requiring reporting of security breaches apply to a breach of data affecting an estate. What obligation does the executor have to the beneficiaries or to the estate if they have not exercised appropriate caution when handling data? It is clear that banks and other financial institutions have an affirmative duty to disclose security breaches and provide retribution to clients in the form of identity theft protection; there is no counterpart for law firms (although there is a large uptick in cybersecurity policies and insurance riders for security breaches). Indeed, many attorneys may be unfamiliar with the ethical opinions of their own state bar associations with respect to the use of cloud-based storage devices.[44] While most states do not have specific requirements, 20 states have issued opinions on the ethical use of cloud-based storage and require attorneys to use reasonable care in doing so. Under these recommendations, attorneys should ensure complete ownership of their data at all times and that access is continually unhindered. Likewise, these recommendations suggest that attorneys should always follow client instructions regarding the storage of their data and that clients provide permission for the transmission or storage of data to a cloud-based system. While this makes sense in the context of a closed IT-server based system, it does not reflect the reality of most practices today, where mobile devices and public Wi-Fi systems may be used to transmit data or communications. This vulnerability could lead to significant repercussions if the data were breached.

Executors and fiduciaries, indeed all representatives and advisors, need to be aware of the increasing risks of cyber crime and take active steps to protect their data. The best mindset to take is that a breach will happen and how can you ensure that damage is minimal. This can include the use of dedicated storage sites with highly sophisticated encryption technology, creating dedicated websites for clients which allow them to have more secure emails and communications, continued use of monitoring systems for spyware and malware and, with the rise of ransom ware, regular and continual downloads of material for backups to ensure that a ransom ware virus does not result in an unexpected cost to the estate.[45]

SUGGESTED ACTION ITEMS

First and foremost, start talking about the issue of digital assets with your clients. Some clients may already have a process in place, or at least a listing of passwords. This will make it easier to suggest the addition of language to their documents and perhaps allow them to formalize their process with an inventory and more comprehensive approach to the management of these assets over time. At a minimum, all clients should be encouraged to inventory their digital assets and create records of passwords, login verifications and note, in particular, what email accounts are tied to these various assets (does your bank account reset to your Apple account or your Gmail account?). Where appropriate, they should establish succession plans with the providers directly (e.g., the Facebook ''last contact'' option or the Gmail ''transfer on death'' authorizations). Further, these inventories should be maintained on a regular basis and in a safe location. Physical form is often preferable to electronic, as counter-intuitive as that may seem, to ensure information remains protected.

Recognizing that few people will ever keep an inventory[46] up to date, at the death of the individual, the executor will have to triage the digital assets and decide what to address first. In an effort to help prioritize, consider:

1. *What pays the bills?* With more bills paid online, or through automatic debits to bank accounts or credit cards, an immediate action for an executor should be on securing and updating billing information for various credit cards, online accounts, and any attendant cash outflows. In addition to keeping the lights on and the water flowing, this will ensure the executor can attend to the cybersecurity and identity theft protection concerns as well.

2. *What income is pending?* While we are conditioned to look for last paychecks and dividend income, executors need to consider other forms of income (or outflow) including sites like EBay, Etsy, PayPal, etc. Securing access to Bitcoin wallets, a growing asset among certain age brackets and increasingly seen as a viable currency, is also

[44] https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

[45] http://www.totaldigitalsecurity.com/blog.

[46] For sample inventories, see www.digitaldeath.com.

ISSN 0148-8295

important. Knowing where a decedent may have had accounts is also critical, especially now that financial accounts can be opened entirely online and without any physical records being created.

3. *What information needs to be kept "alive" and accessible?* Email and social media accounts can be shut down for lack of activity. At the same time, cybersecurity concerns mandate that these accounts be controlled quickly and effectively to minimize the risk of identity theft. The executor should be able to keep appropriate information available to complete the estate process and effectuate any possible transfers or deletion of the data.
4. *What information needs to be backed up?* Clients should be encouraged to make a habit of creating physical backups of their online accounts. With the rise in ransom ware and cyber crime, executors have become an easy target.[47] These backups also ensure that the executor may not have to grapple with access to social media accounts if the information (photos, archived posts or tweets, etc.) is already on backup storage disks that the client owns.
5. *What can be shut down or deleted?* Most of us are borderline hoarders when it comes to our digital media. Providing clear guidance to an executor to permit the deletion or termination of online accounts can avoid any potential liability for these actions. Obviously if there is an open legal matter, a need for the information for taxes or for actions necessary to wind up the affairs of a decedent, then the data or accounts should be retained. In the case of incapacitated individuals, it is better to keep assets and accounts intact until there is clarity as to what can be accessed.[48]

Many advisors opt to engage in ''pre-death'' audits with all clients as a matter of practice — running through the asset values and specific accounts that will transfer to various beneficiaries upon death. Incorporating the digital discussion into these audits can highlight potential areas of value (domain names, client lists, email addresses, etc.) and where a post-mortem handbook on what to do with the information would be needed. All practitioners should begin to incorporate digital language in their documents and increase the use of revocable trusts in case of disability to ensure access (if not for general ease of administration of the other more tangible assets).

Today, an executor will have to find and manage property interests of an ephemeral nature, with an uncertain value. The executor's access to the assets is often limited (if it exists at all) and governed by a unilateral contract that may be governed by international laws. As technology continues to shape our lives and communication, the area of digital assets will take on a heightened importance for planners and advisors. Expanding your template documents to include standard language authorizing access and encouraging clients to begin the inventory process can be an important first step for many advisors. With the rapid change in digital asset legislation, it is important to monitor the activity in your jurisdiction as well. Finally, recognizing that cyber-breaches will happen and encouraging your clients to plan for this loss of information can mitigate the potential cost of a hacking.

---

[47] http://www.darkreading.com/vulnerabilities—-threats/ransomware-will-spike-as-more-cybercrime-groups-move-in/d/d-id/1324720?utm_source=hs_email&utm_medium=email&utm_content=27482291&_hsenc=p2ANqtz-_iKYgSwZbLKTLq5nyqSFxbf_N_wSGwQIABdvSxl6QtubDO8WCCMK3NiyUzvR0eWBupxQSuyNNZSaKERIsps9ms7-09CG8Gk2sosyH0TD4orjDTVqs&_hsmi=27482291.

[48] http://www.sfgate.com/business/article/Check-from-a-scammer-bounces-victim-into-jail-2553957.php.

ISSN 0148-8295