MURTHA CULLINA

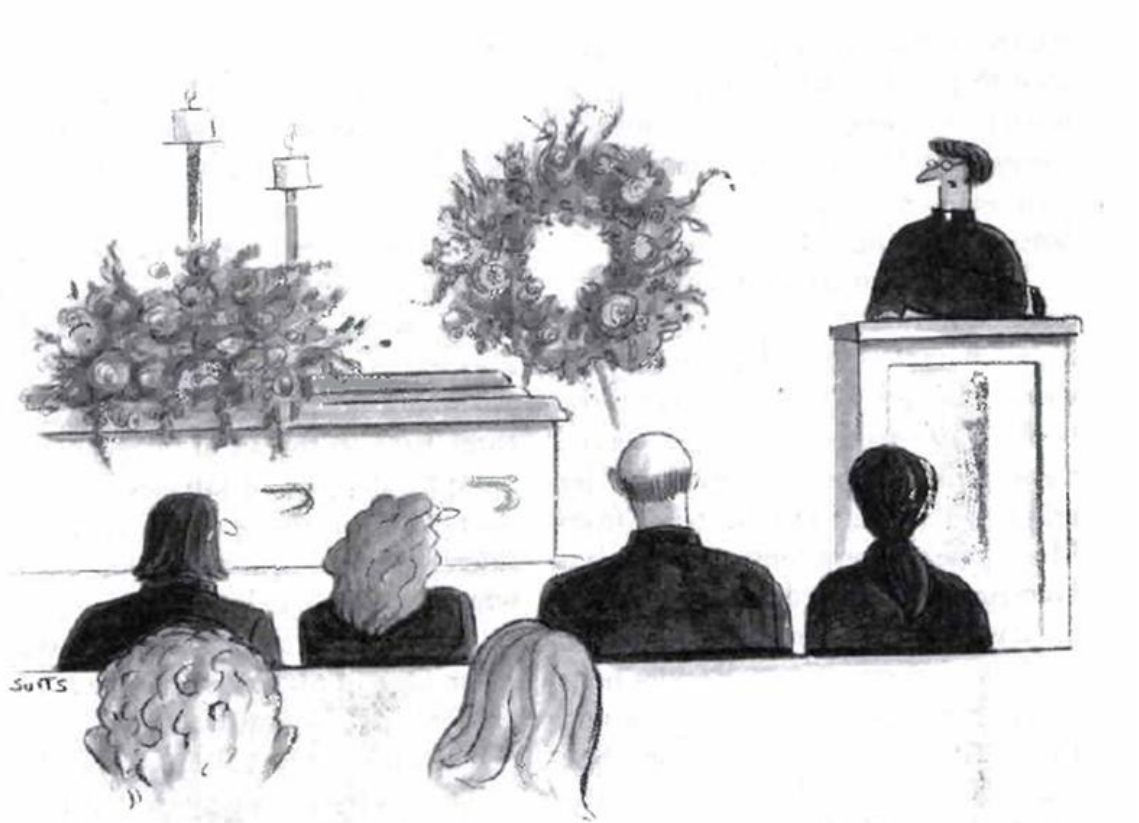
FIRMA 31st Risk Management Training Conference
Breakout Session, 2:30 to 3:30 pm

Fiduciary Access to Digital Assets

Suzanne B. Walsh
860.240.6041 | swalsh@murthalaw.com

Wednesday, May 24, 2017

The Future?



"If anyone's interested in taking over Ed's Instagram account, see me after the service."

Or, the present

A judge takes a “selfie” as he follows a procession of judges in to the houses of parliament in London

And that is no joke

MasterCard has confirmed that it will start accepting "selfies" and fingerprint recognition as an alternative to passwords when verifying ID's for online payments.

MasterCard has rolled out the technology in the UK and 11 other European countries including Spain, Germany and Finland, and plans to bring it worldwide next year.

MURTHA CULLINA

Digital Assets are stored in accounts and on those devices

Why Worry About Fiduciary Access to Digital Assets?

- The majority of people use computers, e-mail, and many use cloud based storage services.
- Of the federal privacy and computer fraud and abuse laws, only one mentions fiduciaries
- Federal Privacy Law Prohibits disclosure of certain electronic communications content without account holder's lawful consent
- Digital assets have significant value

Revised UFADAA (2015)

- **Revised UFADAA Endorsements:**

- Association of American Retired Persons
  Center for Democracy and Technology
  Facebook
  Google
  National Academy of Elder Law Attorneys
- **Enactments** (25): Arizona, Colorado, Connecticut, Florida, Hawaii, Idaho, Illinois, Indiana, Maryland, Michigan, Minnesota, Nebraska, New York, North Carolina, North Dakota, Ohio, Oregon, South Carolina, South Dakota, Tennessee, Utah, Virginia, Washington, Wisconsin, Wyoming
- **2017 Introductions** (19): Alabama, Alaska, Arkansas, District of Columbia, Georgia, Iowa, Kansas, Maine, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Jersey, New Mexico, Rhode Island, Texas, Vermont, West Virginia

Challenges to Fiduciary Access to Digital Assets

- Outdated state probate codes
- Passwords and Encryption
- Federal and state privacy, computer fraud and data protection laws
- Terms of Service Agreements/Privacy Policies Governing Accounts

Passwords and Encryption

- Passwords and encryption, or a software feature, may block fiduciary access to data.
- Example: Apple's iOS 9 auto-erase feature, if enabled, prevents passcode-guessing. After 10 incorrect passcodes, it permanently destroys the data in the device.
- The FBI reportedly paid over $1.3 million to access the San Bernardino shooter's iPhone 5C after this feature encrypted locally stored data.
- Apple was contesting a federal court order that it assist the FBI in neutralizing this feature of its software.

Passwords and Encryption

- Apple case did not involve 4th Amendment.
- Technology companies are increasingly using encryption to protect customers' accounts and devices.
- **It is vitally important to mention the importance of passcodes to clients with Apple devices and iCloud accounts.**

Federal Privacy Laws

- 4th Amendment provides citizens with a strong expectation of privacy in their homes: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause...."
- 4th Amendment prevents government from searching homes without probable cause and a search warrant.

Federal Privacy Laws

- Persons using computer networks at home have the same expectation of privacy, but a computer network is not physically located or being accessed within computers, or in homes, so it is not protected by the 4th amendment.
- To fill that gap, Congress enacted the Stored Communications Act ("SCA") in 1986, as a part of the Electronic Communications Privacy Act ("ECPA"). The SCA is codified as 18 U.S.C. Sections 2701-2711.

Federal Privacy Laws

- The privacy protections of the SCA prohibit certain providers of public communications services from disclosing the contents of user's communications to a government or nongovernment entity (different rules apply to each), except under limited circumstances which are akin to the "warrant" required under the Fourth Amendment.

The Stored Communications Act

- If an e-mail provider only provides it to specific people (such as employees or students) and not to the general public, that provider is not subject to the SCA and cannot use its provisions as a shield against a fiduciary's request for copies of communications or access to an account.
- However, a "private" e-mail provider (school, employer) may have other legitimate grounds for refusing fiduciary access.

Fiduciary Access under the SCA

- SCA prohibits ISP's from divulging EC contents unless 1 of 2 relevant exceptions applies. ISP's face civil damages of at least $1,000 per ECPA violation.
- **Exception 1** allows disclosure to the recipient/addressee of the EC or to the recipient/addressee's **Agent**.
- **Exception 2** allows disclosure of the EC to third parties with the "**lawful consent**" of either its sender or recipient/addressee.
- There is evidence that Congress intended authorized agents to be able to authorize disclosure of the contents of electronic communications.
- Senate Report No. 99-541 on ECPA, taken from the comments to § 2702 (page 37) says: "Either the sender or the receiver can directly **or through authorized agents** authorize further disclosures of the contents of their electronic communication."

The SCA only Protects EC Content (such as e-mails)

- Providers are allowed to divulge *non-content* information such as the user's name, address, connection records, IP address, and account information.
- The **subject line of an email** has been held to be content (Optiver case).
- Social media account contents (photos, videos, posts) not readily accessible to the public are probably all "communications" protected by the SCA.

- Public posts are not protected.

SCA Fiduciary Cases

- 2013—Yahoo!, Inc. refuses to grant Massachusetts fiduciaries access to decedent's email account; Massachusetts appellate court refuses to enforce the CA forum designation provision in its adhesive TOSA provisions; but the underlying issue of fiduciary access is pending before the SJC.

SCA Fiduciary Cases (continued)

- In 2012, Facebook successfully quashes a fiduciary's subpoena request for access to the content of model Sahar Daftary's account; court declines to rule that the executor could supply her "lawful consent" to the disclosure under federal law.

Civil Liability for SCA Violations

- A federal jury in Massachusetts awarded a plaintiff significant monetary damages in a civil action brought under the SCA. Cheng v Romo, 2012 WL 6021369, at *1–3 (D. Mass. Nov. 28, 2012)
- Despite very thin (or nonexistent) testimony to support the damage claim, the jury awarded the plaintiff $450,000 for an unauthorized intrusion into an email account.

Civil Liability for SCA Violations

- Other courts have held that evidence of *actual damages* is required in an SCA case, and have refused to award statutory damages for a violation.
- Vista Marketing, LLC v Burkett, 812 F.3d 954, 975 (11th Cir. 2016).

State, Federal CFAA's

- 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.
- For example, Connecticut criminalizes "unauthorized access" to a computer system, which occurs when "knowing that [a person] is not authorized to do so, he accesses or causes to be accessed any computer system without authorization."
- If the account holder expressly authorized the fiduciary to access her computers, it is unlikely that such computer access violates the CFAA.

Computer Fraud and Abuse Acts (TOSA violations)

- Even if the fiduciary has the user's permission or passwords, the fiduciary may still be breaking the law. Access to a user's online account requires accessing the provider's or another vendor's computer, which requires *the service provider's* further authorization.
- If the provider's TOSA prohibits third parties from accessing the account, when the fiduciary uses a shared password to access the account, he violates the TOSA and thereby exceeds his authorized access *to the service provider's system*. Technically, this violates the CFAA.

Password Sharing

- The easiest way to provide for access to most digital assets during incapacity or after death is by simply sharing a password with a trusted friend or family member.

Terms of Service Agreements "TOSA's"

- Almost no one reads TOSA's when setting up their online accounts, according to a 2016 research study.
- UConn researchers added provisions to a fake website's TOSA disclosing that a user's data would be shared with the NSA and indicating that the user's firstborn child would be taken as payment for using the site. 98% of the 543 unknowing users agreed. http://today.uconn.edu/2016/08/privacy-paradox/
- *See* Terms of Service Didn't Read at https://tosdr.org/

CFAA's and TOSA violations

- Federal prosecutors use the CFAA to prosecute defendants based solely on TOSA violations. The Aaron Swartz case was one highly publicized example of such prosecution. He was a self-described internet activist who committed suicide in 2013, while facing prosecution for impermissibly downloading 4.8 million academic articles from the JSTOR digital library system.

Aaron Swartz

CFAA's and TOSA violations

- Federal court decisions conflict as to whether or not a TOSA violation, alone, can support a criminal CFAA conviction.
- In the 2nd Circuit, the "Cannibal Cop" went free despite his violations of the NYPD's TOSA.
- In the 9th Circuit, the cases are seemingly irreconcilable.

Steve Vachani of Power Ventures

CFAA's and TOSA violations

- Bottom line: Password sharing among family members and access by individual fiduciaries has not yet been and most likely will not be prosecuted as a CFAA violation. However, the statute and the cases interpreting it are not clear.

Revised UFADAA Approach; meaning of "digital asset"

- "Digital assets" defined as records that are electronic.
- Example: an online commodities account for purchasing gold bullion. The digital assets covered by Revised UFADAA are records concerning the account, not the gold itself. Ownership of the gold is not affected by the fiduciary's access to records about the account, even though a transfer of title might occur electronically under other law.
- Example: Virtual currency. Revised UFADAA would clarify that fiduciaries have access to it and own it, just as if it were coins or cash.

Applicability: Section 3

- Revised UFADAA applies to custodians of digital assets of users who reside in a state or resided there at death.
- Revised UFADAA inapplicable to digital assets of employers used by employees in the ordinary course of the employer's business
- *Result: No access to decedent or incapable person's work email in most cases.*

Hierarchy: Section 4

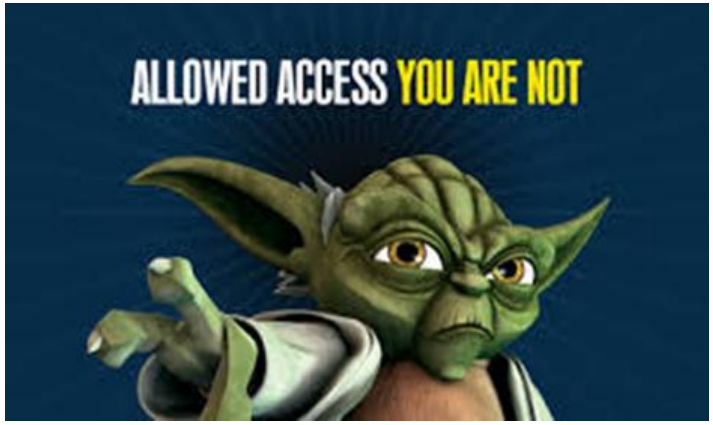
1. On-line tool directions, if offered and modifiable.
2. Directions in will, trusts, powers of attorney or other records.
3. Terms of service agreement provisions (which will govern access for users who do not plan).

TOSA Preserved: Section 5

- This section clarifies that Revised UFADAA does not override a custodian's terms-of-service agreement (**except to give effect to an account holder's express consent as provided in Section 4**), nor does it change or impair a custodian's or user's rights under a TOSA to access and use digital assets.
- Fiduciary does not have greater rights than the user.
- Fiduciary access may be modified or eliminated by a user, by federal law, **or by a TOSA** when the user has failed to plan in a manner recognized by Section 4. CT Act Sec.5(c); NY Sec. 13-A-2.3(c)

Result under Sections 4 & 5

- Fiduciaries for users who fail to plan and who don't use an online tool, store information on a thumb or hard drive, share passwords, or provide for access or disclosure in estate plans may be denied access when the TOSA prohibits it.



Procedure for Disclosing digital assets Section 6

- Gives the custodian 3 options for disclosure:

1. Grant fiduciary full access;
2. Grant partial access to the account sufficient to perform the tasks necessary to discharge duties' or
3. Provide a "data dump" of the information and assets in the user's account.

Procedure for Disclosing digital assets, cont.

- Custodians may charge a reasonable fee
- Custodians need not disclose assets deleted by a user
- If the user directs or the fiduciary requests partial disclosure, the custodian need not comply if segregation imposes an undue burden

Section 6, Procedure for Disclosing digital assets, cont.

- If the custodian considers the request to be unduly burdensome, either it or the fiduciary may ask a court for an order to:
- Disclose a date delimited subset of assets;
- Disclose all or none of the user's assets; or
- Disclose all of the assets to the court for in camera review.

Disclosure of EC Content to Personal Representative: Section 7

Personal representative authority is no longer available by default under Revised UFADAA.

If the user consented to disclosure or if a court directs disclosure, a custodian must disclose EC content, if the personal representative provides: a written request, a death certificate, a certified copy of the letter of appointment, and a copy of the record of the user's consent, if not made in an online tool.

Disclosure of EC Content to Personal Representative, continued

- The personal representative must also provide upon request:
- The number, username or address of the account; evidence linking the user to the account; or a court order finding that the user had the specific account that disclosure would not violate 18 USC 2701, etc.; that the user consented, or that disclosure is reasonably necessary for estate administration.

Disclosure of other Digital Assets to Personal Representative

Unless the user prohibited disclosure or the court otherwise directs, a custodian must disclose all non-EC content digital assets, if the personal representative provides a written request, a death certificate and a letter of appointment. The custodian may also request the information linking the account to the user, and either an affidavit of the necessity of the disclosure or a court order finding that the account was the user's and that disclosure is reasonably necessary. CT Sec. 8; NY Sec. 13-A-3.2

Disclosure of Digital Assets to Agent: Sections 9 & 10

- Unless prohibited by the principal or a court, agent has access to the principal's digital assets, but only to the records (*not the content*) of the principal's electronic communications
- **No default authority** over communications content—principal must expressly grant access, tracking the SCA approach, which requires the user's lawful consent
- Analogy to gifting authority under the UPOAA

Disclosures to Agent

- Whether seeking EC content or other digital assets, Agent must first provide a written request, a copy of the POA, a certification that the power is in effect, and, if requested, the information linking the account to the principal.

Trustee Access when Trustee is original user: Section 11

- Trustee authority over digital assets held in the trust is confirmed, and presumed, when the trustee is the initial user
- This means that the trustee can access the content of each digital asset that is in an account for which the trustee is the original account holder, not necessarily each digital asset held in the trust.

Disclosure of EC Content of Settlor To Trustee

- Section 12 addresses scenarios where there is a successor trustee or a pour over will.
- Trustee can access EC content only if the trust expressly so provides, and the trustee provides a written request, a trust certification, and if the custodian requests, evidence linking the account to the trust.

Disclosure of other digital assets to Trustee

- Unless the trust, a court or the user prohibits it, the custodian must disclose all other digital assets to the trustee who supplies a written request, along with a certified copy of the trust, and if requested, evidence linking the account or asset to the trust. Sec. 13

Disclosure to Conservator (Guardian)

- Permits a court to authorize conservator (guardian) access to digital assets after the opportunity for a hearing, unless the protected person (ward) or court otherwise directs; Section 14
- **Disclosure of EC content not authorized**
- Custodians may be required to disclose non content
- Conservators may ask custodians to suspend or
- terminate accounts for good cause.

Fiduciary Duty and Authority

- Fiduciary authority, except as provided in Section 4, is subject to the TOSA, and also copyright and other law; Sec. 15
- Confirms fiduciary authority over digital assets not held in accounts
- Fiduciary may not impersonate user

Fiduciary Authority

- Confirms that a fiduciary is an authorized user of the decedent, protected person, principal or settlor's property under applicable CFAA's. Sec.15(d)
- Confirms that fiduciary with authority over devices can access files on it and is an authorized user.
- Fiduciaries have express authority to request account termination

Fiduciary Authority

- Subsection 15(e) confirms that the fiduciary is authorized to access digital assets stored on devices, such as computers or smartphones, avoiding violations of state or federal laws on unauthorized computer access.

- Custodians may disclose account information to fiduciary when the information is required to close accounts used to access licensed digital assets. 15(f)

Importance of Planning

- Prevent Financial Loss to Estate
- Avoid Losing the Deceased's Story
- Protect Secrets from Being Revealed
- Avoid identity theft
- Make things easier for families and fiduciaries when clients die or become disabled

Mechanics of Planning

- Client discussion: how does the client use computer and e-mail?
- Digital Asset Authorization and Consent Form
- Durable Powers of Attorney
- Trustee authority over settlor's digital assets
- Commercial DEP Services –see list at http://www.thedigitalbeyond.com/online-services-list/
- Digital Asset Inventory Forms—Industry wants specificity

Terminating or Accessing Accounts

- Mylennium.com has a page of “domain information” which contains an index of many online sites with links to information such as the TOSA, privacy policy, and termination information: https://www.mylennium.com/domaininfo
- Commercial Services such as DCS (Directive Communications Systems) will also assist in identifying and managing all types of online accounts: http://www.directivecommunications.com/what-we-do/

MURTHA CULLINA

Contact Information

Suzanne Brown Walsh, Esq.

860.240.6041

swalsh@murthalaw.com

@walshsuzy on twitter