Western Connecticut Estate & Tax Planning Council, Inc.
Armando's, Bethel, Connecticut
Tuesday, November 17, 2015

Estate Planning for Digital Assets:

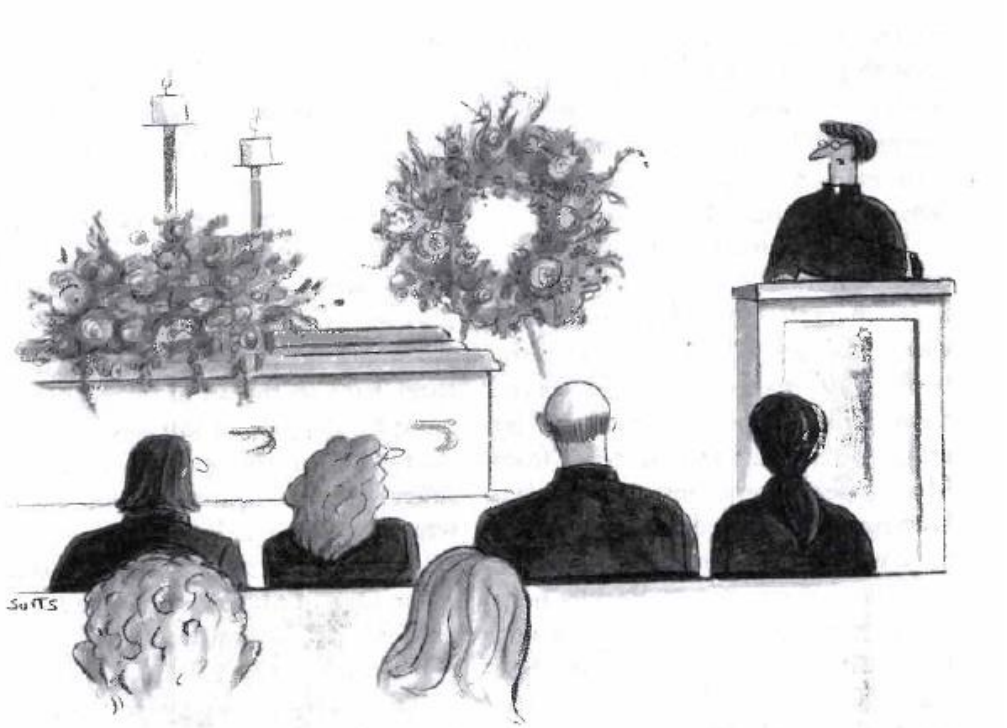
How the Revised Uniform Fiduciary Access to Digital Assets Act Will Help

Suzanne Brown Walsh, Esq.
860.240.6041
swalsh@murthalaw.com

Why Draft a Uniform Law on Fiduciary Access to Digital Assets?

- The majority of people use computers, e-mail, and many use cloud based storage services.
- All of the service providers and custodians have customers in all 50 states, so uniformity will be beneficial
- Only 9 states (CT, DE, ID, OK, IN, LA, RI, NV and VA) have enacted laws specifically granting some type of fiduciary access to digital assets; only Delaware's addresses all fiduciaries and all types of assets
- 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

The future (?)



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

UFADAA (2014)

- The Uniform Law Commission is a nonprofit, unincorporated association that for 124 years has been providing states with nonpartisan, proposed model legislation on various subjects.
- Once a subject is approved as an appropriate one for the ULC, it appoints a drafting committee consisting of commissioners, ABA Advisors and observers.
- The UFADAA drafting committee was approved in 2012, met four times, and the act was approved at its 2014 annual meeting in Seattle.
- UFADAA premised on asset neutrality so its defaults encouraged fiduciary access
- www.uniformlaws.org

UFADAA Enactment

- 27 states introduced UFADAA bills, but none were enacted
- Arkansas, California, Colorado, Connecticut, Florida, Hawaii, Idaho, Illinois, Indiana, Kentucky, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Virginia, Washington
- First enactment by Delaware when HB 345 signed on 8/12/14

Revised UFADAA (2015)

- Despite the high number of bill introductions, UFADAA has not been enacted into law anywhere except Delaware, where a substantially similar law based on a final draft of UFADAA was enacted in 2014. The 2015 bills were blocked by a coalition of internet-based businesses and privacy advocates that opposed certain provisions of UFADAA and offered their own limited model legislation (a version of which was enacted in Virginia).

Revised UFADAA (2015)

- Revised UFADAA was officially approved on July 15, 2015.
- Revisions clarify the application of federal privacy laws, better define the rights and duties of all parties, and give legal effect to an account holder's instructions for the disposition of digital assets.

Challenges to Fiduciary Access to Digital Assets

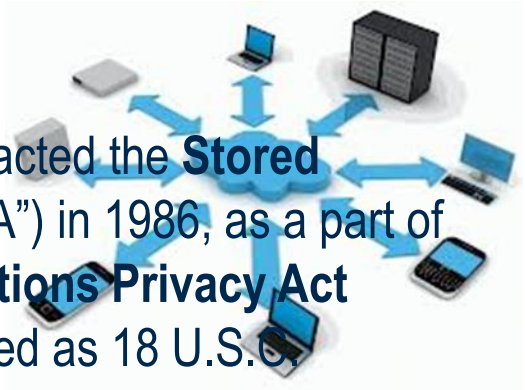
- Outdated state probate codes
- Federal and state privacy, computer fraud and data protection laws
- Passwords and Encryption
- Terms of Service Agreements/Privacy Policies Governing Accounts

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.

Federal Privacy Laws

- 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" EC provider such as an employer may have other, legitimate grounds for refusing fiduciary access.

Fiduciary Access under Federal Privacy Laws

- 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."

Federal Privacy Laws only Protect Content

- Providers are allowed to divulge *non-content* information such as the user's name, address, connection records, IP address, and account information, because the SCA only prohibits the disclosure of the *contents* of communications.
- 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.

Computer Fraud and Abuse Acts

- 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, C.G.S. Section 53a-251 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 with user authorization to access the user's computer(s), the fiduciary may still be breaking the law. Access to a user's online account requires accessing the provider's or another vendor's computers, which requires *the service provider's* further authorization.
- If the provider's TOSA prohibits third parties from accessing the account, when the fiduciary does so, even with the user's authorization, he violates the TOSA and thereby exceeds his authorized access *to the service provider's system*.
- Federal prosecutors have used the CFAA to prosecute defendants *based solely on violations of a website's TOSA*. 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

Computer Fraud and Abuse Acts (TOSA violations)

- Last summer, The Guardian ran an article about Londoners clicking yes on a EULA that required turning over their first-born child in order to use free Wi-Fi: http://tinyurl.com/ng8379o
- *See* Terms of Service Didn't Read at https://tosdr.org/

Computer Fraud and Abuse Acts (TOSA violations)

- A federal jury in Massachusetts awarded a plaintiff significant monetary damages in a civil action brought under the SCA. The defendant had been given the plaintiff's email account password, so she could access it to read consultation reports when the two parties practiced medicine together. When the defendant left the practice and a business dispute arose, she used the plaintiff's unchanged password to access the account for reasons connected to the business dispute. The plaintiff sued, alleging her later access was unauthorized under the SCA. Despite very thin (or nonexistent) testimony to support the damage claim, the jury awarded the plaintiff $450,000 for the unauthorized intrusion.

Fiduciaries Fight Back

- 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 has not yet been decided.

Fiduciaries Fight Back (continued)

- 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

Revised UFADAA Solutions to these Problems

- Defines digital assets
- Applies to personal representatives, conservators (guardians), agents and trustees. Does not apply to employer email systems or assets.
- Defers to account holder/client intent and privacy desires
- Encourages custodian compliance
- Protects fiduciaries, custodians and content providers

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.

Digital Assets, examples

bitcoin

DOMAIN NAME

PLANET CALYPSO

Section 3, Applicability

- Revised UFADAA will govern the actions of a fiduciary or agent acting under a will, trust, or power of attorney executed before, on, or after Revised UFADAA's effective date.
- Revised UFADAA rules will similarly govern all active conservatorship proceedings.

Section 3, Applicability

- 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.*

Section 4 Hierarchy

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).

Section 4-Online Tools, continued

- Section 4 encourages and validates visible TOSA provisions that **allow** third party access (*think beneficiary designation*)
- Facebook's Legacy Contact feature provides limited access to and control of decedent's FB account . Since the Legacy Contact isn't notified until the account is memorialized, he/she has no authority while the AH is alive
- Google's inactive account manager is similar, but can also be triggered by inactivity of a preset duration, so it is available during incapacity

Section 5, TOSA preserved

- This new 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. Act Section 5(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. *See Section 5(c), which says fiduciary access may be eliminated by a TOSA or other means, if the user has not provided direction under Section 4.*

Section 6, Procedure for Disclosing digital assets

- 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.

Section 6, 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

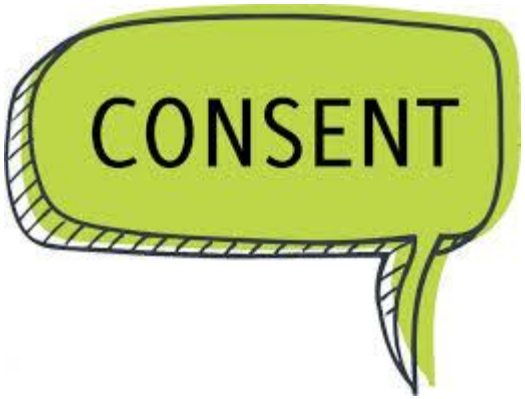
Section 6, Procedure for Disclosing digital assets, cont.

- 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.

Section 7—Disclosure of EC Content to Personal Representative

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.



Section 7—Disclosure of EC Content to Personal Representative

- 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.

Section 8—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.

Sections 9 & 10—Disclosure of Digital Assets to Agent

- 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

Sections 9 & 10—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

Section 11—Trustee Access when Trustee is original user

- 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.

Section 12—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.

Section 13, 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

Section 14—Disclosure to Conservator/Guardian

- Permits a court to authorize conservator access to digital assets after the opportunity for a hearing, unless the protected person or court otherwise directs
- **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.
-

Section 15—Fiduciary Duty and Authority

- Expressly delineates fiduciary duties and limits on fiduciary authority
- Fiduciary authority, except as provided in Section 4, is subject to the TOSA, and also copyright and other law
- Confirms fiduciary authority over digital assets not held in accounts
- Fiduciary may not impersonate user

Section 15—Fiduciary Authority

- Confirms that a fiduciary is an authorized user of the decedent, protected person, principal or settlor's property under applicable CFAA's. Section 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

Section 15—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)

Section 16—Compliance and Immunity

- If fiduciary has access under Revised UFADAA and substantiates authority as specified, custodian must comply with the fiduciary's request for disclosure of the digital asset within 60 days.
- Revised UFADAA thereby mandates what the SCA merely permits if the request is for EC Content.
- Recently a California appellate court held that state law can mandate the disclosure of Electronic Communications: *Negro vs. Navalimpianti USA, Inc., et al.*
- In exchange, Section 16(f) immunizes a custodian who complies with the request.

Privacy

Both the ACLU and the Center for Democracy and Technology have indicated they approve of Revised UFADAA's approach to access from a privacy perspective.

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 and inventory
- Digital Asset Authorization and Consent Form
- Commercial DEP Services –see Digital Beyond list
- Online account succession and authorization—Online Tool

Virtual Currencies- a side note

- In IRS Notice 2014-21, the IRS determined that convertible virtual currencies (like Bitcoin) are *property*, not currency.
- There are over 600 convertible virtual currencies in use, and there are over $3.3 billion worth of bitcoins, alone, in circulation today
- The American Red Cross, the United Way, Greenpeace, and other charities accept donated bitcoins (and other virtual currencies)
- After the November 2013 typhoon that damaged the Philippines, players of the video game EVE Online donated over $190,000 in video game virtual currency to the Red Cross

Virtual Currencies as donations

- If charitable donor "mines" the bitcoins, treated as OI property (deduct at cost basis up to the 50% AGI limitation if a public charity, not an attractive charitable gift).
- If donor did not "mine" bitcoins, treated as CG property
  - If bitcoins held long-term, deductible at full FMV with no tax on the appreciation, up to the 30% AGI limitation if it's a public charity (an attractive charitable gift);
  - If bitcoins held short-term, deductible at the lesser of cost basis (generally not attractive if low basis) or FMV, up to the 50% AGI limitation if it's a public charity.
  - IRS Form 8283 is required if you make charitable gifts of bitcoins over $500.
  - If donor makes charitable gifts using bitcoins totaling over $5,000 in one calendar year, a qualified appraisal is required.

Contact Information

Suzanne Brown Walsh, Esq.
860.240.6041
swalsh@murthalaw.com