WHITE PAPER

PROPOSED ENACTMENT OF CHAPTER 740, FLORIDA STATUTES

I. SUMMARY

The proposed legislation is a result of a study by the Digital Assets Committee of The Real Property, Probate and Trust Law Section of The Florida Bar of recent work on a Uniform Fiduciary Access to Digital Assets Act. The proposal would add a new Chapter to the Florida Statutes that follows the proposed uniform act.

Under present Florida law, there is no legislation on fiduciary access to digital assets, only criminal laws regarding access to stored communications. The purpose of this act is to vest fiduciaries with the authority to access, control, or copy digital assets and accounts. The Florida Fiduciary Access to Digital Assets Act ("FFADAA") addresses four different types of fiduciaries: personal representatives of decedents' estates, guardians of the property of minors or incapacitated persons, agents acting pursuant to a power of attorney, and trustees.

II. CURRENT SITUATION

As the number of digital assets held by the average person increases, questions surrounding the disposition of these assets upon the individual's death or incapacity are becoming more common. These assets range from online gaming items to photos, to digital music, to client lists. And these assets have real value: according to a 2011 survey from McAfee, Intel's security-technology unit, American consumers valued their digital assets, on average, at almost $55,000.[1] Few holders of digital assets and accounts consider the fate of their online presences once they are no longer able to manage their assets. There are millions of Internet accounts that belong to decedents. Some Internet service providers have explicit policies on what will happen when an individual dies, others do not; even where these policies are included in the terms of service, most consumers click through these agreements. Few laws exist on the rights of fiduciaries over digital assets.

The **current federal legislation** that dictates access to digital assets is buried in the Stored Communications Act ("SCA") and the Computer Fraud and Abuse Act ("CFAA"), both passed in 1986, with only minor revisions since. The CFAA and similar state laws impose criminal penalties and perhaps civil liability too for the unauthorized access of computer hardware, devices, and stored data. These laws are explained in more detail below.

---

[1] Kelly Greene, *Passing Down Digital Assets*, WALL STREET JOURNAL (Aug. 31, 2012), http://goo.gl/7KAaOm.

Under **current Florida law**, Florida has enacted statutory counterparts to the provisions of the SCA and located them in Chapter 934, entitled "Security of Communications"[2] and in Chapter 815, entitled “Florida Computer Crimes Act”. There is no legislation on fiduciary access to digital assets.

A minority of **other states** has enacted legislation on fiduciary access to digital assets, including Connecticut, Idaho, Indiana, Oklahoma, Rhode Island, Nevada, and Virginia, and the existing statutes grant varying degrees of access to different types of digital assets. In addition, numerous other states have considered, or are considering, legislation. Existing legislation differs with respect to the types of digital assets covered, the rights of the fiduciary, the category of fiduciary included, and whether the principal’s death or incapacity is covered.

The **National Conference of Commissioners on Uniform State Laws** at its annual conference this July passed the **Uniform Fiduciary Access to Digital Assets Act** (the “UFADAA”). The Act specifically addresses how a fiduciary addresses digital assets. The commissioners on the drafting committee received input from estate attorneys, educators, and lawyers with expertise in various areas of the law affected by digital assets, advisors from the American Bar Association, representatives from service providers, such as Facebook and Yahoo, policy counsel from NetChoice (a trade association of eCommerce businesses and on-line consumers), and General Counsel from the State Privacy and Security Coalition, Inc. (which is comprised of 20 communications, technology, and media companies).[3]

The UFADAA took into account the **Supremacy Clause of the U.S. Constitution**. According to the Supremacy Clause, "This Constitution, and the laws of the United States which shall be made in pursuance thereof.... *shall be the supreme law of the land,* and the judges in every state shall be bound thereby, anything in the Constitution or laws of any State to the contrary, notwithstanding."[4] The Supreme Court has ruled that a federal law that conflicts with a state law "preempts" the state law and that state laws that conflict with federal law are "without effect."[5] Due to the Supremacy Clause and the Supreme Court’s interpretation, one major challenge in drafting the uniform act was that it does not directly conflict with existing federal law and could survive a constitutional challenge.[6]

It is what the **SCA** *does not specifically address* that gave rise to the UFADAA proposed state law that the Uniform State Laws Commissioners believed can be legally interpreted as filling in the gaps of the SCA, as opposed to conflicting with it. The SCA was originally written to provide Fourth Amendment-like[7] privacy protection for certain types

---

[2] *Tracey v. State, 69 So.3d 992* (Fla. 4th DCA 2011).

[3] “Surf the Evolving Web of Laws Affecting Digital Assets” Bissett, W. and Kauffman, D. 41 Estate Planning No. 4 April 2014.

[4] U.S. Const. Art. VI (Emphasis added.)

[5] Maryland v. Louisiana, 451 U.S, 725 (1981).

[6] “Surf the Evolving Web” at 34.

[7] The Fourth Amendment to the U.S. Constitution protects the "people’s rights to be secure in their houses, *papers, and effects,* against unreasonable searches and seizures." (Emphasis added.)

of email communications, social networking accounts, and other digital assets stored on a remote server. "The SCA attempts to modernize the reasonable expectation of privacy provided by the Fourth Amendment and later the Supreme Court to include two types of online services, "electronic communication services" and "remote computing services". To provide this privacy protection, the SCA limits the ability of the government to *compel disclosure* of both "non-content" information (i.e., logs of email communications including addresses of recipient/senders (analogous to the envelope of a letter)) as well as the "content" (what is inside the letter). The SCA also limits the ability of those internet service providers ("ISPs") that are "subject to" the SCA to reveal "content" information to non-government entities."[8] In general, the SCA states that certain service providers are permitted to disclose "non-content" information of electronic communications and files to anyone except the government without the consent of the user. However, a service provider *may* divulge the "content" of an electronic communication to a non-government entity *only* when the account holder lawfully consents.[9]

Like the SCA, the **CFAA** similarly protects against anyone who "intentionally accesses a computer without authorization or exceeds authorized access." Neither the SCA nor the CFAA specifically provides for or denies a fiduciary access to electronic and stored communications. In essence, even if consent was granted to a fiduciary, current federal law does not acknowledge the potential for such a vested right.[10]

The UFADAA uses well-established, existing law for non-digital probate assets in order to provide **a fiduciary the right to "step into the shoes"** of a decedent to manage digital assets. Because the interest to properly administer both non-digital and digital estate assets are similar, a fiduciary should be granted the same authority over both types of property. Because the fiduciary has the same authority as the deceased account holder (no more and no less), the fiduciary is "authorized" by the deceased account holder as required under the two federal statutes (the SCA and CFAA) that prohibit unauthorized access.

The UFADAA was also drafted in light of the fact that deceased account holders likely registered with on-line services for email, on-line purchases, photo sharing, on-line banking, and a long list of other items now done on-line by first consenting to a terms-of service agreement ("TOSA"). The UFADAA recognized that in most situations the account holder likely consented to the TOSA by clicking "I agree" without ever reading it. These TOSAs generally describe the account holder's rights in using the service, how personal information will be protected, the conditions on information sharing, and account holder's rights (if any) upon death. The UFADAA has taken into account a service provider's possible refusal to grant fiduciary access simply because the deceased account holder consented to (a likely unread) blanket TOSA by writing the uniform act such that fiduciary access, by itself, will not be deemed a violation of a TOSA or deemed an unauthorized transfer of an account.[11]

---

[8] "Surf the Evolving Web" at 34 (citations omitted).
[9] 18 U.S.C. section 2702(b)(3).
[10] "Surf the Evolving Web" at 34 (citations omitted).
[11] "Surf the Evolving Web" at 34 (citations omitted).

Because of issues like the federal Supremacy Clause and the interest of ISPs in differing jurisdictions, the Florida drafting committee closely adhered to the careful analysis and drafting set forth within the UFADAA, deviating from the proposed uniform law minimally, only where necessary to comport with Florida law.

III. EFFECT OF PROPOSED CHANGES

A. **Effect of the Proposed Changes.** It is important to understand that the goal of the FFADAA is to remove barriers to a fiduciary's access to electronic records and that the federal and state substantive rules of fiduciary, probate, trust, banking, security, and agency law remain unaffected by FFADAA. The act applies only to fiduciaries that act in compliance with their fiduciary powers. It distinguishes the authority of fiduciaries—which exercise authority subject to this act only on behalf of the account holder—from any other efforts to access the digital assets. Family members or friends may seek such access, but, unless they are fiduciaries, their efforts are subject to other laws and are not covered by this act.

This Act follows mirros the UFADAA because a uniform approach among states will provide certainty and predictability for courts, account holders, fiduciaries, and ISPs. The uniform act gives states precise, comprehensive, and easily accessible guidance on questions concerning fiduciaries' ability to access the electronic records of a decedent, protected person, principal, or a trust. Additionally, ISPs have participated in the drafting of the UFADAA and, presumably, find the proposed act to be acceptable.

The general goal of the FFADAA is to facilitate fiduciary access while respecting the privacy and intent of the account holder. It adheres to the traditional approach of trusts and estates law, which respects the intent of the account holder and promotes the fiduciary's ability to administer the account holder's property. With regard to the general scope of the act, the act's coverage is inherently limited by the definition of "digital assets." The act applies only to electronic records. The term does not include the underlying asset or liability unless it is itself an electronic record.

B. The act is divided into **twelve sections**.

1. **Section 740.101** contains the short title of the Act.

2. **Section 740.201** contains general provisions and definitions, including those relating to the scope of the fiduciary's authority.

The definitions of "agent", "guardian", "court", "electronic", "fiduciary", "governing instrument", "person", "personal representative", "power of attorney", "principal", "record", "trustee", "ward", and "will" are based on those found in applicable Florida law, such as the Florida Probate Code and Florida Powers of Attorney Act.

UFADAA Uniform Act	Florida Statutes
Section .201 Definitions	
(2) Agent	709.2102(1)
(6) Court	731.201(7)
(9) Electronic	709.2102(5)
(12) Fiduciary	739.102(6), 738.102 (4), 733.817, 518.10
(13) Governing Instrument	732.2025(4)
(14) Guardian	744.604(6)
(16) Person	1.01(3)
(17) Personal Representative	731.201(28)
(18) Power of Attorney	709.2102(7)
(19) Principal	709.2102(9)
(20) Record	709.2102(13)
(23) Trustee	731.201(39)
(24) Ward	744.102(22)
(25) Will	731.201(40)

The other definitions are new for this Act, although the definition of digital service comes from the White House Digital Government Strategy: http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf. The definition of "contents" is adapted from 18 U.S.C. § 2510(8); the definition of "electronic communication" is adapted from the language of 18 U.S.C. §§ 2510(12) and 2702(a)(1) and (2); the definition of "electronic communication service" is drawn from 18 U.S.C. 2510(15); and the definition of "remote computing service" is adapted from 18 U.S.C. § 2711(2), to help ensure the Act's compliance with federal law.

The Act includes a definition for "catalogue of electronic communications." This is designed to cover log-type information about an electronic communication. The term "content of an electronic communication" is adapted from 18 U.S.C. § 2510(8), but it refers only to information that is not readily accessible to the public because, if the information were readily accessible to the public, it would not be subject to the privacy protections of federal law under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 et seq. See S. Rep. No. 99-541, at 36 (1986). When the privacy protections of federal law under ECPA apply to the content of an electronic communication, the ECPA's legislative history notes the requirements for disclosure: "Either the sender or the receiver can directly or through authorized agents authorize further disclosures of the contents of their electronic communication." S. Rep. No. 99-541, at 37 (1986)).

ECPA does not apply to private e-mail service providers, such as employers and educational institutions.[12]

[12] See 18 U.S.C. §2702(a)(2); James D. Lamm, Christina L. Kunz, Damien A. Riehl, & Peter John Rademacher, *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. Miami L. Rev. 385, 404 (2014) (available at: http://goo.gl/T9jX1d).

A "custodian" includes any internet service provider as well as any other entity that provides or stores electronic data of an account holder. The term "carries" means engaging in the transmission or switching of electronic communications. See 47 U.S.C. § 1001(8). A custodian does not include most employers because an employer typically does not have a terms-of-service agreement with an employee. Any digital assets created through employment generally belong to the employer.

Example -- Fiduciary access to an employee email account. D dies, employed by Company Y. Company Y has an internal email communication system, available only to Y's employees. D's personal representative, R, believes that D used Company Y's email system for some financial transactions that R cannot find through other means. R requests access from Company Y to the emails.

Company Y is not a custodian subject to the act. Under Section .201(6), a custodian must carry, maintain or store an account holder's digital assets. An account holder, in turn, is defined under Section .201(1) as someone who has entered into a terms-of-service agreement. Company Y, like most employers, did not enter into a terms-of-service agreement with D, so D was not an account holder.

"Digital assets" include products currently in existence and yet to be invented that are available only electronically. Digital assets include electronically-stored information, such as: 1) any information stored on a computer and other digital devices; 2) content uploaded onto websites, ranging from photos to documents; and 3) rights in digital property, such as domain names or digital entitlements associated with online games.[13] Both the catalogue and content of an electronic communication are covered by the term "digital assets."

The fiduciary's access to a record defined as a "digital asset" does not mean that the fiduciary is entitled to "own" the asset or otherwise engage in transactions with the asset. Consider, for example, funds in a bank account or securities held with a broker or other custodian, regardless of whether the bank, broker, or custodian has a brick-and-mortar presence. This Act affects records concerning the bank account or securities, but does not affect the authority to engage in transfers of title or other commercial transactions in the funds or securities, even though such transfers or other transactions might occur electronically. The Act reinforces the right of the fiduciary to access all relevant electronic communications and the online account that provides evidence of ownership. Thus, an entity may not refuse to provide access to online records any more than the entity can refuse to provide the fiduciary with access to hard copy records.

The definition of "electronic communication" is adapted from the language of 18 U.S.C. §§ 2510(12) and 2702(a)(1) and (2); the definition of "electronic-communication service" is drawn from 18 U.S.C. § 2510(15); and the definition of "remote-computing service" is adapted from 18 U.S.C. § 2711(2), to help ensure the

[13] See Lamm, et al, supra, at 388.

Act's compliance with federal law. Electronic communication is a subset of digital assets and covers only the category of digital assets subject to the privacy protections of the ECPA. For example, material stored on a computer's hard drive is a digital asset but not an electronic communication.

A "fiduciary" under this chapter occupies a status recognized by Florida law, and fiduciaries' powers under the chapter are subject to the relevant limits established by other state laws.

The "terms-of-service agreement" ("TOSA") definition relies on the definition of "agreement" found in UCC § 1-201(3) and that found in UCC § 1-201(b) (3) ("the bargain of the parties in fact, as found in their language or inferred from other circumstances, including course of performance, course of dealing, or usage of trade"). It refers to any agreement that controls the relationship between an account holder and a custodian, even though it might be called a terms-of-use agreement, a click-wrap agreement, a click-through license, or a similar term. State and federal law determine capacity to enter into a binding terms-of-service agreement.

3. **Section 740.301** establishes the rights of personal representatives. A personal representative is presumed to have access to all of the decedent's digital assets unless that is contrary to the decedent's will or to other applicable law.

This section establishes the default rule that the personal representative is authorized to access all of the decedent's digital assets other than material covered by the ECPA. The subsection clarifies the difference between fiduciary authority over digital assets other than electronic communications protected by ECPA, and authority over ECPA-covered electronic communications. For electronic communications, subsections (1) and (2) establish procedures that cover: first, the ECPA-covered content of communications and, second, the catalogue (logs and records) that electronic communications service providers may release without consent under the ECPA. Federal law distinguishes between the permissible disclosure of the "contents" of a communication, covered in 18 U.S.C. § 2702(b), and of "a record or other information pertaining to a" subscriber or customer, covered in 18 U.S.C. § 2702(c).[14]

Content-based material can, in turn, be divided into two types of communications: those received by the account holder and those sent. Material when the account holder is the "addressee or intended recipient" can be disclosed either to that individual or to an agent for that person, 18 U.S.C. § 2702(b)(1), and it can also be disclosed to third parties with the "lawful consent" of the addressee or intended recipient. 18 U.S.C. § 2702(b)(3). Material for which the account holder is the "originator" can only be disclosed to third parties with the account holder's "lawful consent." 18 U.S.C. § 2702(b)(3). (Note that, when the account holder is the addressee or intended recipient, material can be disclosed under either § 2702(b)(1) or (b)(3), but that when the account holder is the originator, lawful consent is required.) By contrast to content-based material, non-content material

[14] See Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105 (2009).

can be disclosed not only with the lawful consent of the account holder but also to any person other than a governmental entity (which would presumably include fiduciaries). This information includes material about any communication sent, such as the addressee, sender, date/time, and other subscriber data, what this Act defines as the "catalogue of electronic communication". (Further discussion of this issue and examples are set out in the comments to Section .701, *infra*.)

4. **Section 740.401** establishes the rights of guardians. A guardian may access the assets pursuant to letters of guardianship or a court order.

This section establishes that the guardian must be specifically authorized by the court to access the ward's digital assets and electronic communications. Each of the different levels of access must be specifically granted by court order. The requirement for express authority over digital assets does not limit the fiduciary's authority over the underlying "bricks and mortar" assets, such as a bank account. As a legislative enacting matter, the meaning of the term "hearing" will vary, depending on a state's procedures.

Section .401 is comparable to Section .301. It responds to the concerns of ISPs who believe that the Act should be structured to clarify the difference between fiduciary authority over digital assets other than electronic communications protected by federal law (the ECPA) and fiduciary authority over ECPA-protected electronic communications. Consequently, this Act sets out procedures that cover all digital assets as well as the catalogue of electronic communications (logs and records) that providers may release without consent under ECPA, and then addresses ECPA-covered communications.

Under Section .401, the guardian has the same power over digital assets as the account holder. The guardian must exercise authority in the best interests of the ward pursuant to Chapter 744.

5. **Section 740.501** establishes the rights of agents acting pursuant to a power of attorney. An agent acting pursuant to a power of attorney is presumed to have access to all of a principal's digital assets not subject to the protections of other applicable law; if another law protects the asset, then the power of attorney must explicitly grant access.

This section establishes that the agent has default authority over the principal's digital assets and the records, other than the contents, of the principal's electronic communications. When the principal does not want the agent to exercise this authority, then the power of attorney must explicitly prevent an agent from doing so.

With respect to the contents of electronic communications, the agent must be specifically authorized by the principal to access the contents of the principal's electronic communications. Because a power of attorney contains the consent of the account holder, ECPA should not prevent the agent from exercising authority over the content of electronic communications. There should be no question that an explicit delegation of authority in a power of attorney constitutes authorization from the account holder to access digital assets, and provides "lawful consent" to allow disclosure of electronic

communications from an electronic communication service or a remote computing service pursuant to applicable law. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

The uniform law commissioners considered whether the authority over digital assets and electronic communications should be a default power. They decided that the power to access the contents of electronic communications must be expressly granted, because when expressed and not default, it satisfies the lawful consent requirement of ECPA. The agent has default authority over other digital assets under the Act.

6. **Section 740.601** establishes the rights of trustees. A trustee may access any digital asset held by the trust unless that is contrary to the terms of the trust or to other applicable law

Access to digital assets, including the contents of the electronic communications, is presumed with respect to assets for which the trustee is the initial account holder. A trustee may have title to digital assets and electronic communications when the trust itself becomes the account holder of a digital asset held by the trust, and when the trustee becomes an account holder for trustee business, situations addressed in subsection (1).

Subsection (2) addresses situations involving either an inter vivos transfer of a digital asset into a trust or transfer via a pour-over will of a digital asset into a trust. There should be no question that holding property in trust form constitutes authorization from the account holder for the trustee to access digital assets, including both the catalogue and contents of the electronic communications, and this provides "lawful consent" to allow disclosure of electronic communications from an electronic communication service or a remote computing service pursuant to applicable law. Nonetheless, subsection (2) distinguishes between the catalogue and contents of electronic communications in case there are any questions about whether the form in which property – transferred into a trust - is held constitutes lawful consent. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization, and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

The underlying trust documents and the Florida Trust Code will supply the allocation of responsibilities between and among trustees.

7. **Section 740.701** contains provisions relating to the rights of the fiduciary to access digital assets.

This section clarifies that the fiduciary has the same authority as the account holder if the account holder were the one exercising the authority (note that, where the account holder has died, this means that the fiduciary has access as of the hour before the account holder's death). This means that the fiduciary's authority to access the digital asset is the same as the account holder except where, pursuant to subsection (2), the account holder has explicitly opted out of fiduciary access. Of course, in exercising its

responsibilities, the fiduciary is subject to the duties and obligations established pursuant to Florida law and is liable for breach of those duties.

This issue concerning the parameters of the fiduciary's authority potentially arises in two situations: 1) the fiduciary obtains access to a password directly from the account holder, as would be true in various circumstances such as for the trustee of an inter vivos trust or someone who has stored passwords with a digital locker and those passwords are then transmitted to the fiduciary; and 2) the fiduciary has obtained access pursuant to this Act.

The fiduciary does not, however, obtain power over any digital assets if that property was illegally obtained by the account holder. Note that even if the digital asset were illegally obtained by the account holder, the fiduciary would still need access in order to handle that asset appropriately. There may, for example, be tax consequences that the fiduciary would be obligated to report.

The section also provides that control by a fiduciary should not be considered a transfer that would violate the anti-transfer terms of a terms-of-service agreement. Finally, the fiduciary has the same responsibilities as the account holder more generally. For example, a fiduciary cannot delete an account if this would be fraudulent. Similarly, if the account holder could challenge provisions in a terms-of-service agreement, then the fiduciary is similarly able to do so.[15]

Subsection (1) is designed to establish that the fiduciary is authorized to exercise control over digital assets in accordance with other applicable laws. The language mirrors that used in Title II of the ECPA, known as the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.* The subsection clarifies that the fiduciary is "authorized" under the two federal statutes that prohibit unauthorized access to computers and computer data, the SCA and the CFAA,[16] as well as pursuant to any comparable state laws criminalizing unauthorized access.[17]

The Stored Communications Act contains two potentially relevant prohibitions.

(a) 18 U.S.C. § 2701(a), which concerns access to the digital assets, makes it a crime for anyone to "intentionally access without authorization a facility through which

---

[15] See *Ajemian v. Yahoo!, Inc*., 987 N.E.2d 604 (Mass. 2013).

[16] Stored Communications Act, 18 U.S.C. § 2701 *et seq*. (2006); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*. (2006); *see, e.g.,* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Allan D. Hankins, Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295 (2012).

[17] *See Computerized Hacking and Unauthorized Access States Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 21, 2009), http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx; Christina Kunz, Peter Rademacher & Lucie O'Neill, 50 State Survey of Unauthorized Access (2012) (on file with the Committee and available on the Google Drive); James D. Lamm, et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. Miami L. Rev. __ (2013), http://lawreview.law.miami.edu/wp-content/uploads/2011/12/The-Digital-Death-Conundrum-How-Federal-and-State-Laws-Prevent-Fiduciaries-from-Managing-Digital-Property.pdf.

an electronic communication service is provided" as well as to "intentionally exceed an authorization to access that facility." Thus, someone who has authorization to access the facility is not engaging in criminal behavior. Moreover, this section does not apply to "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user."[18]

(b) 18 U.S.C. § 2702, "Voluntary disclosure of customer communications or records," concerns actions by the service provider. It prohibits an electronic communication service or a remote computing service from knowingly divulging the contents of a communication that is stored by or carried or maintained on that service unless disclosure is made (among other exceptions) "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient" or "with the *lawful consent* of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service."[19] The statute permits disclosure of "customer records" that do not include content, either with lawful consent from the customer or "to any person other than a governmental entity."[20] Thus, unlike the contents, the provider is permitted to disclose the non-content "records" of the electronic communications to anyone except the government, and may disclose to the government with the customer's lawful consent or in certain emergencies.

The Computer Fraud and Abuse Act prohibits unauthorized access to computers. 18 U.S.C. § 1030. Like the SCA, the CFAA similarly protects against anyone who "intentionally accesses a computer without authorization or exceeds authorized access." 18 U.S.C. § 1030(a).

Florida laws prohibit unauthorized access. See Chapters 815 and 934, Florida Statutes.

By defining the fiduciary as an authorized user: 1) the fiduciary has authorization to access the files under the *first* section of the SCA, 18 U.S.C. § 2701, as well as under the CFAA; and 2) the fiduciary has "the lawful consent" of the originator/subscriber so that the provider can voluntarily disclose the files pursuant to the *second* relevant provision of the SCA, 18 U.S.C. § 2702. Moreover, this language should be adequate to avoid liability under the Florida unauthorized access laws.

Subsection (4) reinforces the concept that the fiduciary "steps into the shoes" of the account holder, with no more – and no fewer – rights. For example, the TOSA controls the rights of the account holder (settlor, principal, incapacitated person, decedent). The Act does not permit the account holder's fiduciary to override the TOSA in order to make a digital asset or collection of digital assets "descendible," although it does preserve the rights of the fiduciary to make the same claims as the account holder.[21]

---

[18] 18 U.S.C. §§ 2701(a), (c)(2).
[19] 18 U.S.C. § 2702(b)(1), (3) (emphasis added).
[20] 18 U.S.C. § 2702(c)(2) and (6).
[21] See *Ajemian v. Yahoo!, Inc*., 987 N.E.2d 604 (Mass. 2013); David Horton, *Indescendibility*, 102 Calif. L. Rev. __ (forthcoming 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311506.

Subsection (5) is designed to clarify that the fiduciary is authorized to access digital assets stored on equipment of the decedent, ward, principal, or settlor, thereby superseding Florida laws on unauthorized access to the equipment.

Example 1 – Access to digital assets by personal representative. D dies with a will that is silent with respect to digital assets. D has a bank account for which D received only electronic statements, D has stored photos in a cloud-based Internet account, and D has an e-mail account with a company that provides electronic-communication services to the public. The personal representative of D's estate needs access to the electronic bank account statements, the photo account, and e-mails.

The personal representative of D's estate has the authority to access D's electronic banking statements and D's photo account, which both fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to the personal representative, then the bank and the photo account service must give access to the personal representative when the request is made in accordance with Section .801. If the TOSA permits D to transfer the accounts electronically, then the personal representative of D's estate can use that procedure for transfer as well.

The personal representative of D's estate is also able to request that the e-mail account service provider grant access to e-mails sent or received by D; ECPA permits the service provider to release the catalogue to the personal representative. The service provider also must provide the personal representative access to the content of an electronic communication sent or received by D if the service provider is permitted under 18 U.S.C. Section 2702(b) to disclose the content. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 2 – Access to digital assets by guardian. C is seeking appointment as the guardian for P. P has a bank account for which P received only electronic statements, P has stored photos in a cloud-based Internet account, and P has an e-mail account with a company that provides electronic communication services to the public. C needs access to the electronic bank account statements, the photo account, and e-mails.

Without a court order that explicitly grants access to P's digital assets, including electronic communications, C has no authority pursuant to this Act to access the electronic bank account statements, the photo account, or the e-mails. Based on law outside of this Act, the bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 3 – Access to digital assets by agent. X creates a power of attorney designating A as X's agent. The power of attorney expressly grants A authority over X's

digital assets, including the content of an electronic communication. X has a bank account for which X receives only electronic statements, X has stored photos in a cloud-based Internet account, and X has a game character and in-game property associated with an online game. X also has an e-mail account with a company that provides electronic-communication services to the public.

A has the authority to access X's electronic bank statements, the photo account, the game character and in-game property associated with the online game, all of which fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to A as X's agent, then the bank, the photo account service provider, and the online game service provider must give access to A when the request is made in accordance with Section .801. If the TOSA permits X to transfer the accounts electronically, then A as X's agent can use that procedure for transfer as well.

As X's agent, A is also able to request that the e-mail account service provider grant access to e-mails sent or received by X; ECPA permits the service provider to release the catalogue. The service provider also must provide A access to the content of an electronic communication sent or received by X if the service provider is permitted under 18 U.S.C. Section 2702(b) to disclose the content. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 4 – Access to digital assets by trustee. T is the trustee of a trust established by S. As trustee of the trust, T opens a bank account for which T receives only electronic statements. S transfers into the trust to T as trustee (in compliance with a TOSA) a game character and in-game property associated with an online game and a cloud-based Internet account in which S has stored photos. S also transfers to T as trustee (in compliance with the TOSA) an e-mail account with a company that provides electronic-communication services to the public.

T is an original account holder with respect to the bank account that T opened, and T has the ability to access the electronic banking statements. T, as successor account holder to S, may access the game character and in-game property associated with the online game and the photo account, which both fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to T as trustee, then the bank, the photo account service provider, and the online game service provider must give access to T when the request is made in accordance with Section .801. If the TOSA permits the account holder to transfer the accounts electronically, then T as trustee can use that procedure for transfer as well.

T as successor account holder of the e-mail account for which S was previously the account holder is also able to request that the e-mail account service provider grant access to e-mails sent or received by S; the ECPA permits the service provider to release the catalogue. The service provider also must provide T access to the content of an electronic communication sent or received by S if the service provider is permitted under 18 U.S.C. Section 2702(b) to disclose the content. The bank may release the catalogue of

electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 5 – Access notwithstanding terms in a TOSA. D, who is domiciled in Florida, dies. D was a professional photographer who stored valuable digital photos in an online storage account provided by C. P is appointed by a court in Florida to administer D's estate. P needs access to D's online storage account to inventory and appraise D's estate assets and to file D's estate tax return. During D's lifetime, D entered into a TOSA with C for the online storage account. The choice-of-law provision selects the law of state Y to govern the contractual rights and duties under the TOSA. A provision of the TOSA prohibits fiduciary access to the digital assets of an account holder, but D did not agree to that provision by an affirmative act separate from D's assent to other provisions of the TOSA. FFADAA has been enacted but no similar law has been enacted by state Y. Because P's access to D's assets is fundamental to carrying out P's fiduciary duties, a court should apply subsections (b) and (c) of this Act to void the TOSA provision prohibiting P's access to D's online account, even though the TOSA selected the law of state Y to govern the contractual rights and duties under the TOSA.

8. **Section 740.801** addresses compliance.

Subsection (1) allows a fiduciary to request access, control, or a copy of the digital asset. The term "control" means only the ability to move (unless prohibited by copyright law) or delete that particular asset. A fiduciary's control over a digital asset is not equivalent to a transfer of ownership or a laundering of illegally obtained material. Thus, this subsection grants the fiduciary the ability to access electronic records, and the disposition of those records is subject to other laws. For example, where the account holder has an online securities account or has a game character and in-game property associated with an online game, then the fiduciary's ability to sell the securities, the game character, or the in-game property is controlled by traditional probate law. The act is only granting access and "control" in the sense of enabling the fiduciary to do electronically what the account holder could have done electronically. Thus, if a TOSA precludes online transfers, then the fiduciary is unable to make those transfers electronically as well.

Example – Fiduciary control over a digital asset. D dies with a will disposing of all D's assets to D's spouse, S. E is the personal representative for D's estate. D left a bank account, for which D only received online statements, and a blog.

E as personal representative of D's estate has access to both of D's accounts and can request the passwords from the custodians of both accounts. If D's agreement with the bank requires that transferring the underlying title to the account be done in person, through a hard copy signed by the account holder and the bank manager, then E must comply with those procedures (signing as the account holder) and cannot transfer the funds in the account electronically. If the TOSA for the blog permitted D to transfer the blog electronically, then E can make the transfer electronically as well.

Subsection (3) establishes 60 days as the appropriate time for compliance. If applicable law other than this act does not prohibit the custodian from complying, then the custodian must grant access to comply.

9. **Section 740.901** grants immunity to custodians.

This section establishes that custodians are protected from liability when they act in accordance with the procedures of this Act and in good faith. The types of actions covered include disclosure as well as transfer of copies.

10. **Section 740.1001** establishes the relation with the Electronic Signatures in Global and National Commerce Act.

11. **Section 740.1101** establishes the applicability of this Act. This Act applies in situations in which a decedent dies testate or intestate, as well as a guardianship.

This Act does not change the substantive rules of other law, such as agency, banking, guardianship, contract, copyright, criminal, fiduciary, privacy, probate, property, security, trust, or other applicable law except to vest fiduciaries with authority, according to the provisions of this Act, to access, control, or copy digital assets of a decedent, ward, principal, settlor, or trustee.

12. **Section 12** establishes the effective date.

IV. FISCAL IMPACT ON STATE AND LOCAL GOVERNMENTS

The proposal does not have a fiscal impact on state or local governments. In fact, it should decrease the risk of unauthorized access to digital assets from the fiduciaries appointed by account holders and would provide certainty and predictability for courts, account holders, fiduciaries, and Internet service providers.

V. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR

The proposal does not have a direct economic impact on the private sector.

VI. CONSTITUTIONAL ISSUES

There appear to be no constitutional issues raised by this proposal.

VII. OTHER INTERESTED PARTIES

Criminal Law Section, State law enforcement and state attorney offices who track and enforce privacy and cyber crimes.
Florida Bankers Association
Business Law Section
Trial Lawyers Association