COMMONWEALTH OF MASSACHUSETTS

SUPREME JUDICIAL COURT

NO. SJC-12237

ROBERT AJEMIAN & ANOTHER
Plaintiffs-Appellants

v.

YAHOO INC.
Defendant-Appellee.

ON APPEAL FROM A JUDGMENT OF
THE NORFOLK PROBATE AND FAMILY COURT DEPARTMENT

BRIEF OF *AMICI CURIAE* NETCHOICE AND THE INTERNET ASSOCIATION

James R. McCullagh, WSBA 27744
jmccullagh@perkinscoie.com
Ryan T. Mrazik, WSBA 40526
rmrazik@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
(206) 359-8000

Joseph Aronson, BBO 022070
jaronson@bonnerkiernan.com
Bonner Kiernan Trebach & Crociata LLP
200 Portland Street, 4th Floor
Boston, MA 02114
(617) 426-3900

February 21, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*

NetChoice is a trade association of leading e-commerce businesses and online companies.[1] It promotes value, privacy, and trust in internet business models. NetChoice works to prevent and remove unnecessary barriers on new businesses, make the internet more accessible and ubiquitous, and promote e-commerce, which is the new backbone of economic growth. NetChoice's members provide services including email, direct message, social network, blog, and comments services to tens of thousands of individuals in Massachusetts, allowing users to connect with one another and access online goods and services.

The Internet Association ("IA") represents 40 of the world's leading internet companies.[2] Its mission is to foster innovation, promote economic growth, and

---

[1] NetChoice members include 21st Century Fox, Alibaba Group, AOL, DJI, DRN, eBay, the Electronic Retailing Association, Expedia, Facebook, Google, HomeAway, Liberty Interactive Corporation, Lyft, Overstock.com, PayPal, Travel Tech, Verisign, Vigilant Solutions, and Yahoo.

[2] The Internet Association's members include Airbnb, Amazon, Coinbase, DoorDash, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Google, Groupon, Handy, IAC, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, Reddit, Salesforce.com, Snap, Spotify, SurveyMonkey, Ten-X, TransferWise, TripAdvisor, Turo, Twitter, Uber Technologies, Inc., UpWork, Yahoo, Yelp, Zenefits, and Zynga.

empower people through the free and open Internet. As the voice of the world's leading internet companies, the IA helps ensure that all stakeholders understand the benefits the internet brings to our economy and society in general. To realize these benefits, it is important that fair and appropriate consideration be given to the impact that overly broad interpretations of state and federal laws have on the ability of innovators, including IA members, to scale and grow.

Protecting user privacy, enabling user choice, and being able to rapidly innovate are core tenets of successful online businesses. Enabling and respecting user privacy and choice is particularly important for electronic communications. Congress has expressly recognized the privacy interests that users have in their electronic communications and, in enacting the Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"), set forth only limited circumstances when a provider may disclose their users' communications.

Upsetting Congress's balanced regime with an implied exception allowing disclosure of a deceased person's communications to people not of the person's choosing would undercut users' confidence in the privacy of their communications and slow the economic

growth that has made the technology industry in the United States the most successful in the world.

NetChoice and IA therefore have a direct and vital interest in the issues before this Court. They respectfully submit this brief in response to this Court's Announcement of January 5, 2017.

INTRODUCTION AND SUMMARY OF ARGUMENT

Amici are responding to the Court's invitation for amicus briefs addressing "[w]hether the Federal Stored Communications Act, 18 U.S.C. § 2702, prohibits disclosure -- by an entity that provides electronic mail message services -- of the contents of a deceased account holder's account, including the communications contained therein, to the administrators of his or her estate." Mass. R. App. P. 17.

Amici agree with Appellee Yahoo! Inc. ("Yahoo") that the Stored Communications Act ("SCA") does not permit electronic mail message services to disclose the contents of a deceased person's account to the administrators of his or her estate unless an enumerated statutory exception allows the provider to do so. Amici also agree with Yahoo that the statutory exceptions in the SCA permitting voluntary disclosures should be read narrowly because a narrow reading is consistent with the SCA's purpose and structure.

Amici's members offer online communication services to billions of people throughout the world. They depend on user trust in their services and the privacy protections afforded to users' communications. In enacting the SCA, Congress comprehensively

legislated in this area with a focus on protecting user privacy. This focus ensures that users' choices about when and to whom to disclose their electronic communications remain intact even after death.

The best indication of when and with whom a deceased person meant to share her electronic communications is how she shared them while alive. These communications, which include all types of content--email, other messages (private, public, and group), as well as photos, videos, and comments--can include the most sensitive and personal topics in people's lives. When stored in password-protected accounts and shared only with people the user chooses, the user's privacy desires are clear. These choices should be respected even after death.

Rejecting a novel exception for personal representatives or estate administrators to access those communications will effectuate user privacy and choice, guard against unauthorized disclosure, protect providers from burdensome requests to pry into users' accounts, and encourage industry to develop services that continue to enable user privacy and choice.

Indeed, in a recent NetChoice poll on this exact issue, more than 70 percent of Americans agreed that

they want their online communications and photos to remain private after they die, unless they provide consent prior to their death to share the communications with others. Seventy percent of Americans also felt that the law should err on the side of privacy when someone dies without documenting their preferences about how to handle her private communications and photos. This is not surprising: the overwhelming majority of the American public want their private communications to remain private.

The SCA is in lock step with these policies and this empirical evidence. It prohibits service providers from disclosing users' communications except under narrow circumstances. Neither the consent nor agency exceptions, as relied on by Appellant Personal Representatives ("Personal Representatives"), permits providers to disclose stored communications to court-appointed estate administrators.

The Superior Court correctly concluded that there is no evidence of consent and that the lawful consent exception is not satisfied by imputed or inferred consent. Similarly, there is no evidence that decedent created an agency relationship with Personal Representatives while he was alive for the purpose of

allowing access to his stored electronic communications. Regardless, construing the consent and agency exceptions narrowly is both consistent with congressional intent and necessary to enable Amici's members to operate their services to honor the privacy choices and expectations of their users.

Recently, states have begun legislating fiduciary rights to digital assets. The Uniform Law Commission passed the Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA"), which has been enacted in various forms in approximately 20 states. Although Massachusetts has not enacted a law to address this issue, states that have done so generally recognize that their laws cannot override the SCA and require express consent from the account owner before a personal representative may receive a decedent's stored electronic communications. Further, the SCA and these laws vest service providers with the discretion to determine the required form of consent, if any, based on the nature of their services.

For each of these reasons as further set out below, Amici strongly support Yahoo's position and respectfully submit that this Court should affirm the reasoned decision of the Superior Court.

ARGUMENT

A. Protecting User Privacy and Choice is of Paramount Importance.

1. The Focus and Purpose of the SCA is to Protect User Privacy.

The SCA "focus[es] on protecting the privacy of the content of a user's stored electronic communications." *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, 217 (2d Cir. 2016). Protecting the privacy of user communications is the "object[] of the statute's solicitude." *Id.* (citing *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247, 267 (2010)). And although the SCA does provide when a user's communications can be disclosed, the statutory language and history "suggest[] a legislative focus on the privacy of stored communications." *Id.*

Indeed, Congress's motivation in enacting the SCA was "to protect the privacy of our citizens" by imposing federal statutory presumptions that codify citizens' expectations of privacy in "new forms of telecommunications and computer technology." S. Rep. No. 99-541, at 5 (1986). The SCA "creates a zone of privacy to protect internet subscribers from having their personal information wrongfully used and

publicly disclosed by 'unauthorized private parties'." *Bower v. Bower*, 808 F. Supp. 2d 348, 350 (D. Mass. 2011) (quoting S. Rep. No. 99-541, at 3 (1986)).

This unmistakable focus on user privacy serves two important purposes. First, it gives users of online services the confidence that their communications will be protected from third-party access except in limited circumstances, thereby increasing users' trust in the services. *See O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1445 (2006). Second, it alleviates "legal uncertainty" and the "severe administrative burdens" that technology providers would face in responding to third-party requests seeking a user's communications content. *Id.* at 1446. This, in turn, enables companies like Amici's members to focus on innovating, developing, improving, and launching communications services that are widely used in Massachusetts and around the world.

In discussing the need for these protections for electronic communications, Congress recognized that technical advancements were changing the ways people communicated. It also noted the potentially damaging effect that the accompanying legal uncertainty could have on peoples' privacy and technological advances:

> "[T]his legal uncertainty poses potential problems in a number of areas. First, it may unnecessarily discourage potential customers form [sic] using such systems, and encourage unauthorized users to obtain access to communications to which they are not party. . . . But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right."

H.R. Rep. No. 99-647, at 19 (1986). The pace of technical advancements has only accelerated since then, and Congress's prescient observation that technology was changing how people communicated is just as accurate today as it was in 1986. The concern and need to protect user privacy in stored electronic communications remains, and Congress clearly enshrined these protections in the SCA.

2. The SCA's Privacy Protections Are More Important Than Ever.

The SCA's protections are more important than ever because the privacy concerns presented by modern electronic communications are different in quality and quantity from any type of communication in the past. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 390 (2014) (Prior to the arrival of cheap, online storage "few records were created, few records were stored, and therefore, few records could be obtained [by third parties under

the ECPA]."). Not only are there myriad ways to communicate through Amici's members' services, such as text messages, email, social networks, voice messages, photo and video sharing, comments, and collaborative creation of content, but the volume of stored communications has exploded. *See id.* at 392 ("[A] typical Gmail user stores more than seventeen thousand emails in her account at any given time."). The ease with which people can store a substantial volume of their most personal data for long periods of time is unprecedented and requires special treatment.

Further, how people protect their electronic communications materially differs from the ways that they typically protect traditional physical assets, such as a diary or box of letters or photos stored under a bed or tucked away in a closet. A person expects that those physical assets will be found and reviewed upon death. But with a password-protected email, social media, or other communications account, a person assumes that its stored communications will not be discovered because they are accessible only by logging into a password-protected account. Users therefore expect that their electronic accounts and communications will retain the level of privacy that

they have configured during their lifetimes.

Empirical evidence supports this expectation. A poll commissioned by NetChoice revealed unequivocally that "[m]ore than 70 percent of Americans think that their private online communications and photos should remain private after they die--unless they gave prior consent for others to access." *See Privacy Afterlife Poll*, NetChoice, https://netchoice.org/library/decedent-information/#poll (last visited Feb. 20, 2017). Seventy percent of survey respondents also felt that "the law should err on the side of privacy when someone dies without documenting their preference about how to handle their private communications and photos." *See id.* Other key findings include:

- 65 percent of Americans said that it violates their privacy if their private communications and photos are shared without their consent.
- Only 15 percent of Americans believed that estate attorneys and executors should have the discretion to decide what happens to private communications when no prior consent was given.
- Three out of four Americans said that they would either make arrangements for friends and family to have access to private communications or didn't want anyone to access them.

- Fewer than 10 percent of Americans would want to give consent for an estate attorney or executor to have full access to private communications.

Id.

Importantly, users' expectation that their electronic accounts and communications will retain the level of privacy that they configured during their lifetimes accounts only for the interests of the deceased user, not the interests of the people with whom the deceased user communicated. Those persons' privacy interests remain and the wholesale release of stored communications in a decedent's account can have significant and life-altering consequences. One does not have to think long to imagine the effect that revealing private communications related to a deceased user or a still-living party to a communication could have if the communication concerns sexual orientation, medical issues, private relationships, or any number of other deeply personal matters.

These significant issues are eloquently addressed by the SCA-compliant practice that permits a provider to disclose envelope information to a personal representative to enable that representative to seek the communications from the other parties to the communication. *See* 18 U.S.C. § 2702(c)(6). This is

the process Yahoo followed in this case, and it is the process this Court should endorse, while rejecting Personal Representatives' attempt at overreaching.

3. The Law Should Respect the Choices Users Make While Alive.

The best way to protect user privacy and choice is to respect the privacy choices that the decedent made when she was alive. Every day, users decide which people to include on an email (or not), who to share a social network post with, and when and where to comment online. Those decisions are personal and it is inappropriate for an estate administrator or the judicial system to second-guess and effectively revise a person's choices simply because she has died.

A number of service providers give the people who use their services options to designate when and how others may access their electronic communications when they die. Some services provide tools to users to designate who and how individuals should receive their electronic communications after their death or prolonged period of inactivity. *See, e.g., Inactive Account Manager*, Google, https://www.google.com/settings/account/inactive (last visited Feb. 20, 2017). Further, users can designate in their will or

other documents their wishes as to their electronic accounts as well as their tangible assets. Finally, if communications might be needed to administer an estate and a deceased user has not chosen to disclose them by one of those means, a provider can, consistent with the SCA, disclose the envelope information for a communication (when and with whom a communication was made), and the communications can then be sought from other parties to the communications.

B. Consistent with the Purpose of the SCA and Users' Expectations, the Court Should Not Expand the Consent and Agency Exceptions under the SCA.

Personal Representatives argue they are entitled to the contents of decedent's email account because (1) they can consent on the decedent's behalf to its disclosure or (2) as court-appointed personal representatives of decedent's estate, they are the decedent's agents. Accepting either theory would erode the privacy protections that underpin the SCA and require the Court to create a novel exception to the SCA. This Court should decline that invitation.

1. The SCA Prohibits Providers from Disclosing Communications and Permits Disclosures Subject to Only Limited Exceptions.

The SCA starts with the unambiguous premise that access to stored electronic communications is

prohibited unless an enumerated exception applies. 18 U.S.C. § 2701. It also provides that electronic communication services ("ECS") and remote computing services ("RCS") to the public "shall not knowingly divulge to any person or entity the contents of a communication" unless one of eight exceptions applies. 18 U.S.C. § 2702(a); (b)(1)-(8). Courts have thus recognized that the "primary obligations [on providers] created by the SCA protect the electronic communications," and "[d]isclosure is permitted only as an exception to those primary obligations." *Warrant to Search E-Mail*, 829 F.3d at 218; *see also O'Grady*, 139 Cal. App. 4th at 1443 ("[T]here is no pertinent ambiguity in the language of the [SCA]. It clearly prohibits any disclosure of stored email other than as authorized by enumerated exceptions.").

Of the eight exceptions, Personal Representatives argue that the lawful consent and agency exceptions permit service providers to disclose communications content to a court-appointed administrator. 18 U.S.C. § 2702(b)(1), (3). Personal Representatives are wrong because neither exception applies here.

2. Implied or Imputed Consent Are Insufficient Under the SCA and Should Not be Permitted.

a. The SCA Requires Actual Consent.

Section 2702(b)(3) of the SCA permits covered service providers to "divulge the contents of a communication . . . with the lawful consent of the originator or an addressee or intended recipient of such communications, or the subscriber in the case of remote computer service." The Personal Representatives here, and personal representatives or estate administrators in general, are obviously not one of the listed people that can consent to disclosure. The deceased account owner is. Any argument that a personal representative or estate administrator can consent, therefore, rests not on a theory of actual consent, but consent that is implied.

The lawful consent exception in § 2702(b)(3), however, "is not satisfied by consent that is merely constructive, implied in law, or otherwise imputed to the user by a court." *Negro v. Superior Court*, 230 Cal. App. 4th 879, 889 (2014); *see also In re Irish Bank Resolution Corp. Ltd. (in Special Liquidation)*, 559 B.R. 627, 650 (Bankr. D. Del. 2016) ("[C]onsent for the purposes of the SCA 'must be consent in

fact.'") (citation omitted). Expanding the consent exception to disclose content to people with whom the user did not expressly authorize contravenes the clear purpose of the lawful consent exception, which:

> is manifestly intended to invest users with the final say regarding disclosure of the contents of their stored messages while limiting the burdens placed on service providers by the Act. The latter interest is obviously diminished to the extent that the Act is applied in such a way as to embroil service providers in disputes . . . over the legal sufficiency of a user's conduct to constitute consent.

Negro, 230 Cal. App. 4th at 896 (internal citation omitted).

Further, the prohibition on imputing consent has been upheld in the bankruptcy context even when the account at issue is linked to assets disputed in litigation. *Irish Bank Resolution Corp. ("IRBC")*, 559 B.R. at 648. In *IRBC*, the bankruptcy court found that the foreign representatives of a debtor in litigation pending in Ireland were not entitled to compel Yahoo to provide them access to an email account that purportedly included communications relevant to the bankruptcy proceeding. *Id.* at 653-54. The court ordered the account user to turn over the contents of the account, but the user failed to respond. *Id.* at

633-35. The foreign representatives then sought to compel Yahoo to turn over the account records in the user's stead. *Id.* at 634-37.

After analyzing the SCA, the court determined that "courts interpreting the SCA have declined to create an 'implicit exception to the [SCA] for civil litigation,' and have repeatedly found that persons other than the actual subscriber may not give consent to disclose information found in a private email account." *Id.* at 649-50 (quoting *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 730 (9th Cir. 2011)). The court denied the foreign representatives' motion because the court lacked "the authority to compel a service provider to divulge the contents of a private email [account] solely at the request of a third-party after the account user has failed to give his or her consent." *Id.* at 652. The same rationale precludes Personal Representatives' argument here.

b. Requiring Actual Consent and Preserving Provider Discretion Protects Both Users and Providers.

Requiring actual consent effectuates the policy goal of respecting the privacy choices that users made during their lifetimes. It is also reflected in recent efforts by state legislatures to enact the

Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA") to update state fiduciary law for the Internet age. As described by the Uniform Law Commission, the "[r]evised UFADAA provides the legal authority for a fiduciary to manage digital assets in accordance with the user's estate plan, while ensuring that a user's private electronic communications remain private unless the user consented to disclosure." RUFADAA Fact Sheet, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/Revised%202015/Revised%20UFADAA%20-%20Fact%20Sheet%20-%20June%2016%202016.pdf (last visited Feb. 20, 2017).[3]

---

[3] States that have passed a version of RUFADAA include Arizona (Ariz. Rev. Stat. §§ 14-13101 to 14-13118 (2016)); California (Cal. Prob. Code §§ 870-884 (2016)); Colorado (Colo. Rev. Stat. § 15-1-1501 to 15-1-1518 (2016)); Connecticut (Conn. Gen. Stat. § P.A. 16-145 (2016)); Florida (Fla. Stat. §§ 740.001-.09 (2016)); Hawaii (Haw. Rev. Stat. § 556A (2016)); Idaho (Idaho Code § 15-14 (2016)); Illinois (755 Ill. Comp. Stat. §§ 70/1 to /21 (2016)); Indiana (Ind. Code § 32-39-1, 2 (2016)); Maryland (Md. Code, Est. & Trusts §§ 15-601 to -620 (2016)); Michigan (Mich. Comp. Laws § 700.1001-.1018 (2016)); Minnesota (Minn. Stat. § 521A (2016)); Nebraska (Neb. Rev. Stat. § 30-501 to -518 (2015)); New York (N.Y. Est. Powers & Trusts Law § 13-A-1 (2016)); North Carolina (N.C. Gen. Stat. § 36F (2016)); Ohio (HB 432 signed into law on Jan. 4, 2017); Oregon (OR LAWS 2016 Ch. 19); South Carolina (S.C. Code § 62-2-1010 to -1090 (2016)); Tennessee (Tenn. Code § 35-8 (2016)); Washington (Wash. Rev. Code §§ 11.120.010-.120.901 (2016)); Wisconsin (Wis. Stat. § 711 (2016)); and Wyoming (Wyo. Stat. § 2-3-1001 to -1017 (2016)).

Importantly, RUFADAA comports with the disclosure restrictions in the SCA while also prioritizing the user's directions about the disposition of her digital assets. Specifically, the RUFADAA allows fiduciaries to manage digital property like computer files, web domains, and virtual currency in accordance with a user's estate plan. With respect to stored communications, the RUFADAA creates a tiered framework to protect a user's private communications from disclosure in a manner that is contrary to the user's express wishes, consistent with the SCA. Thus, a user's statement through an online tool or, if that is not present, a will, governs the disposition of her assets. If the user has not provided express consent regarding disclosure of stored communications, then the terms of service may apply (if they speak to the issue), but in any case the provider may disclose information only as permitted by the SCA.

This framework recognizes decedents' strong privacy interests in stored electronic communications, while simultaneously providing clear instructions for how estate administrators may obtain the content from a user's electronic communications accounts in a manner consistent with the SCA.

Finally, even when actual consent is present, providers must retain discretion to choose to make a disclosure. Notably, the SCA's consent exception, like the other exceptions of section 2702, is subject to provider discretion. It provides that "[a] provider ... ***may*** divulge the contents of a communication ... with the lawful consent of the originator or an addressee or intended recipient of such communications, or the subscriber in the case of remote computer service." 18 U.S.C. § 2702(b)(3) (emphasis added). "The use of the word 'may' denotes a discretionary power." *Provencal v. Commonwealth Health Ins. Connector Auth.*, 456 Mass. 506, 513 (2010); *Brittle v. City of Boston*, 439 Mass. 580, 594 (2003) ("may" is permissive, not mandatory); *see also United States v. Rodgers*, 461 U.S. 677, 706 (1983) ("The word 'may,' when used in a statute, usually implies some degree of discretion."). In addition, Section 2702 is titled "***Voluntary*** disclosure of customer communications or records," indicating that providers are not obligated to make certain disclosures. 18 U.S.C. § 2702 (emphasis added).

Provider discretion has been recognized by courts and accounts for the varied and constantly developing

nature of communication services. Courts interpreting section 2702 have repeatedly confirmed that "while consent may permit production by a provider, it may not require such a production." *In re Facebook, Inc.*, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012); *see also Schweickert v. Hunts Point Ventures, Inc.*, No. 13-cv-675RSM, slip op. at 20 (W.D. Wash. Dec. 4, 2014) ("Even if the court could compel Plaintiff to consent to the disclosure of some [of] her emails under Rule 34, the providers would still only be permitted, but not required, to turn over the contents under 18 U.S.C. § 2702(b)(3)"]; *State v. Bray*, 383 P.3d 883, 891 (Or. Ct. App. 2016) (noting that "under [the] plain language of 18 USC § 2702(b), disclosure pursuant to exception is discretionary").[4]

Provider discretion recognizes that service providers may have unique ways to verify user identity. For example, in many cases, user identity is verified only by logging in to the account. In such cases, providing a photo ID or death certificate will have no bearing on determining account ownership

[4] Although a provider is not obligated to produce information based on consent, in some situations valid consent coupled with valid legal process may be a basis for disclosure. *See Negro*, 230 Cal. App. 4th at 901-04.

because the provider has no means to determine whether that documentation corresponds to the owner of the account.

Provider discretion also helps protect users against mistake or fraud. Because user verification often occurs by the process of logging in to an account or other pre-defined account recovery methods, providers can detect fraudulent activity, such as when an account identified by a personal representative as belonging to the decedent has been accessed after the date of death. Imputing consent could mistakenly result in people gaining access to accounts or disclosure of content for which the decedent was not actually an owner. Similarly, some services allow for shared accounts. Imputing consent in these cases could result in people gaining access to accounts that remain active and contain the private communications of the shared owners. Other mechanisms for implied or imputed consent are also fraught with the dangers of wrongful access, improper disclosure, and public exposure of a person's private affairs.

3. Court-Appointed Personal Representatives Are Not Agents of the Decedent.

a. A Court-Appointed Representative is Not an "Agent" under the SCA.

As with the consent exception, the agency exception in section 2702(b)(1) should be construed narrowly. The Restatement (Second) of Agency § 14(c) (1958)[5] provides that the agency relationship turns on the principal's "control" over the agent.[6] Amici have not identified any instance where an agency theory has been applied to compel a service provider to divulge the contents of communications to a court-appointed administrator. Indeed, a court-appointed administrator is responsible to the court rather than the deceased user, and a "person appointed by a court

---

[5] The SCA does not specifically define agency, but the Restatement provides guidance and federal courts often look to the Restatement to interpret undefined terms in federal statutes. Further, as noted in Personal Representatives' brief, turning to state law definitions of agency would create potentially unpredictable and inconsistent application of the federal statute.

[6] *See also* Restatement (Third) of Agency § 1.01, comment (f)(1) (2006) ("An essential element of agency is the principal's right to control the agent's actions." "[I]f a person is appointed by a court to act as a receiver, the receiver is not the agent of the person whose affairs the receiver manages because the appointing court retains the power to control the receiver."). If a deceased user did appoint an agent him or herself, the death of either the agent or the principal terminates the agency relationship. Restatement (Third) of Agency § 3.07, (1), (2) (2006).

to manage the affairs of others is not an agent of the others." Restatement (Second) of Agency § 14F (1958).

For example, in *In re Toft*, a U.S. Bankruptcy Court denied a motion to compel service providers to disclose emails of a debtor to an insolvency administrator, holding that the "trustee would not be entitled to such relief," as it would "contravene the protection against disclosure of emails by internet service providers contained in the [SCA]." 453 B.R. 186, 189 (Bankr. S.D.N.Y. 2011). The court held that such relief "is manifestly contrary to U.S. public policy" because it "would directly compromise privacy rights subject to a comprehensive scheme of statutory protection . . . built on constitutional safeguards incorporated in the [U.S. constitution] as well as the constitutions of many States." *Id.* at 198.

The *Irish Bank Resolution Corporation* litigation likewise rejects extending the agency exception to persons appointed by a court. It held "that the SCA and the case law interpreting it do not support the notion of compelling an email service provider to disclose electronically stored information . . . by designating a third-party as the 'subscriber.'" 559 B.R. at 632. Representatives moved to compel

production of a Yahoo account based on the claim that it was the debtor's property, or at minimum contained information related to the debtor's property or financial affairs, arguing that they could stand in the shoes of the subscriber. *Id.* at 636-37, 642.

The court rejected this expansion of the agency exception and declined to find that the representatives could be characterized as the subscriber, noting that they themselves "admitted ... that they were unable to find a single case that supports the notion of designating someone else [other than the account holder] as the subscriber." *Id.* at 651. These cases establish that whether a person qualifies as an "agent" under the SCA is subject to narrow interpretation and applies only to someone to whom a user specifically grants permission to access his or her account. A court-appointed representative would not meet this standard.

b. Classifying Court-Appointed Representatives as Agents Would Undermine User Privacy and Burden Service Providers.

Adopting Personal Representatives' broad interpretation of the agency exception under the SCA would undermine users' privacy and choices in the same

way that adopting their overbroad reading of the consent exception would. Users expect their communications to be sent and shared only with those people they specifically choose. A court designating a representative as a legal "agent" after a user's death and then allowing that "agent" to receive all the deceased user's electronic communications would nullify the choices made by the user during her life.

Moreover, allowing other persons to stand in the shoes of an account holder would impose burdens and risks on service providers. For example, different jurisdictions vest different powers in administrators and require different procedures in the administration of an estate. Providers would have to sort through all those laws and procedures, somehow verify that the sought-after account was properly subject to an estate administrator's request (without being able to contact the accountholder, who would be deceased), and disclose content stored in that account, all while being subject to the risk of potential civil liability for wrongful disclosure. *See* 18 U.S.C. § 2707.

These operational and legal burdens would cause providers to withdraw resources from what they do best--innovating, developing, building, improving, and

providing the best online communications systems in the world--in order to address a patchwork of state laws and the differing obligations imposed by those state laws. Not only will this burden providers, but it is inconsistent with and less protective than the SCA. *See Telecomm. Regulatory Bd. of Puerto Rico v. CTIA-Wireless Ass'n*, 752 F.3d 60, 68 (1st Cir. 2014) (finding state law requiring production of basic subscriber information to the state regulator without any legal process was preempted by the SCA.).

CONCLUSION

In enacting the SCA, Congress struck a careful balance that protects users' privacy and creates clear rules for service providers. That framework, the values of user privacy and choice, and preserving the ability of service providers to develop and offer communications services, counsel strongly in favor of affirming the Superior Court, as Yahoo urges.

The Personal Representatives seek to upend that balance by advancing novel theories that no court has adopted. The right they seek would undercut the SCA's privacy protections and undermine peoples' trust in the online ecosystem: no password or user selection would be strong enough to counteract a contrary wish

by an unchosen administrator. And a user who decides while alive that she does not want her communications disclosed after death would have no means to prevent it. Providers would also face legal uncertainty and the risk that they could be forced, by mistake or fraud, to violate their users' privacy interests.

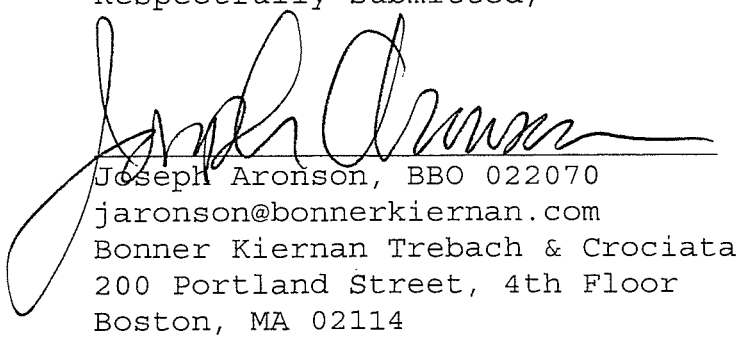
For these reasons, Amici urge the Court to reject Personal Representatives' contention, and affirm the Superior Court.

CERTIFICATE OF COMPLIANCE

The undersigned counsel certifies that this brief complies with the rules of court that pertain to the filing of briefs, including, but not limited to: Mass. R. App. P. 16(a) (6), Mass. R. App. P. 16(e), Mass. R. App. P. 16(f), Mass. R. App. P. 16(h), Mass. R. App. P. 18, and Mass. R. App. P. 20.

DATED: February 21, 2017

Respectfully submitted,



Joseph Aronson, BBO 022070
jaronson@bonnerkiernan.com
Bonner Kiernan Trebach & Crociata LLP
200 Portland Street, 4th Floor
Boston, MA 02114
(617) 426-3900
(F)(617) 426-0380

ADDENDUM

tions Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

(Added Pub. L. 103–414, title II, § 201(a), Oct. 25, 1994, 108 Stat. 4289.)

REFERENCES IN TEXT

The Foreign Intelligence Surveillance Act of 1978, referred to in subsec. (a), is Pub. L. 95–511, Oct. 25, 1978, 92 Stat. 1783, as amended, which is classified principally to chapter 36 (§ 1801 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of Title 50 and Tables.

The Communications Assistance for Law Enforcement Act, referred to in subsecs. (a) and (b), is title I of Pub. L. 103–414, Oct. 25, 1994, 108 Stat. 4279, which is classified generally to subchapter I (§ 1001 et seq.) of chapter 9 of Title 47, Telegraphs, Telephones, and Radiotelegraphs. Sections 102 and 108 of the Act are classified to sections 1001 and 1007, respectively, of Title 47. For complete classification of this Act to the Code, see Short Title note set out under section 1001 of Title 47 and Tables.

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

AMENDMENTS

2002—Pub. L. 107–273, div. B, title IV, § 4005(b), Nov. 2, 2002, 116 Stat. 1812, made technical correction to directory language of Pub. L. 107–56, title II, § 223(c)(2), Oct. 26, 2001, 115 Stat. 295, effective Oct. 26, 2001. See 2001 Amendment note below.

2001—Pub. L. 107–56, title II, §§ 223(c)(2), 224, Oct. 26, 2001, 115 Stat. 295, as amended by Pub. L. 107–273, div. B, title IV, § 4005(b), Nov. 2, 2002, 116 Stat. 1812, temporarily added item 2712.

Pub. L. 107–56, title II, §§ 212(a)(2), (b)(2), 224, Oct. 26, 2001, 115 Stat. 285, 295, temporarily substituted "Voluntary disclosure of customer communications or records" for "Disclosure of contents" in item 2702 and "Required disclosure of customer communications or records" for "Requirements for governmental access" in item 2703.

1988—Pub. L. 100–690, title VII, § 7067, Nov. 18, 1988, 102 Stat. 4405, which directed amendment of item 2710 by inserting "for chapter" after "Definitions" was executed by making the insertion in item 2711 to reflect the probable intent of Congress and the intervening redesignation of item 2710 as 2711 by Pub. L. 100–618, see below.

Pub. L. 100–618, § 2(b), Nov. 5, 1988, 102 Stat. 3197, added item 2710 and redesignated former item 2710 as 2711.

§ 2701. Unlawful access to stored communications

(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 103–322, title XXXIII, § 330016(1)(K), (U), Sept. 13, 1994, 108 Stat. 2147, 2148; Pub. L. 104–294, title VI, § 601(a)(3), Oct. 11, 1996, 110 Stat. 3498; Pub. L. 107–296, title II, § 225(j)(2), Nov. 25, 2002, 116 Stat. 2158.)

AMENDMENTS

2002—Subsec. (b)(1). Pub. L. 107–296, § 225(j)(2)(A), in introductory provisions, inserted ", or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State" after "commercial gain".

Subsec. (b)(1)(A). Pub. L. 107–296, § 225(j)(2)(B), substituted "5 years" for "one year".

Subsec. (b)(1)(B). Pub. L. 107–296, § 225(j)(2)(C), substituted "10 years" for "two years".

Subsec. (b)(2). Pub. L. 107–296, § 225(j)(2)(D), added par. (2) and struck out former par. (2) which read as follows: "a fine under this title or imprisonment for not more than six months, or both, in any other case."

1996—Subsec. (b)(1)(A), (2). Pub. L. 104–294 substituted "fine under this title" for "fine of under this title".

1994—Subsec. (b)(1)(A). Pub. L. 103–322, § 330016(1)(U), substituted "under this title" for "not more than $250,000".

Subsec. (b)(2). Pub. L. 103-322, §330016(1)(K), substituted "under this title" for "not more than $5,000".

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

EFFECTIVE DATE

Section 202 of title II of Pub. L. 99-508 provided that: "This title and the amendments made by this title [enacting this chapter] shall take effect ninety days after the date of the enactment of this Act [Oct. 21, 1986] and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect."

SHORT TITLE OF 1988 AMENDMENT

Pub. L. 100-618, §1, Nov. 5, 1988, 102 Stat. 3195, provided that: "This Act [enacting section 2710 of this title and renumbering former section 2710 as 2711 of this title] may be cited as the 'Video Privacy Protection Act of 1988'."

§ 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) 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;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination.

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108-21, title V, §508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

(Added Pub. L. 99-508, title II, §201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 100-690, title VII, §7037, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 105-314, title VI, §604(b), Oct. 30, 1998, 112 Stat.

Subsec. (b)(2). Pub. L. 103–322, § 330016(1)(K), substituted "under this title" for "not more than $5,000".

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

EFFECTIVE DATE

Section 202 of title II of Pub. L. 99–508 provided that: "This title and the amendments made by this title [enacting this chapter] shall take effect ninety days after the date of the enactment of this Act [Oct. 21, 1986] and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect."

SHORT TITLE OF 1988 AMENDMENT

Pub. L. 100–618, § 1, Nov. 5, 1988, 102 Stat. 3195, provided that: "This Act [enacting section 2710 of this title and renumbering former section 2710 as 2711 of this title] may be cited as the 'Video Privacy Protection Act of 1988'."

§ 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) 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;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108–21, title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 100–690, title VII, § 7037, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 105–314, title VI, § 604(b), Oct. 30, 1998, 112 Stat.

2984; Pub. L. 107-56, title II, § 212(a)(1), Oct. 26, 2001, 115 Stat. 284; Pub. L. 107-296, title II, § 225(d)(1), Nov. 25, 2002, 116 Stat. 2157; Pub. L. 108-21, title V, § 508(b), Apr. 30, 2003, 117 Stat. 684; Pub. L. 109-177, title I, § 107(a), (b)(1), (c), Mar. 9, 2006, 120 Stat. 202, 203; Pub. L. 110-401, title V, § 501(b)(2), Oct. 13, 2008, 122 Stat. 4251.)

AMENDMENTS

2008—Subsecs. (b)(6), (c)(5). Pub. L. 110-401 substituted "section 2258A" for "section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032)".

2006—Subsec. (a). Pub. L. 109-177, § 107(c), inserted "or (c)" after "Except as provided in subsection (b)".

Subsec. (b)(8). Pub. L. 109-177, § 107(b)(1)(A), struck out "Federal, State, or local" before "governmental entity".

Subsec. (c)(4). Pub. L. 109-177, § 107(b)(1)(B), added par. (4) and struck out former par. (4) which read as follows: "to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;".

Subsec. (d). Pub. L. 109-177, § 107(a), added subsec. (d).

2003—Subsec. (b)(5). Pub. L. 108-21, § 508(b)(1)(C), which directed amendment of par. (5) by striking "or" at the end, could not be executed because "or" did not appear at the end. See 2002 Amendment note below.

Subsec. (b)(6). Pub. L. 108-21, § 508(b)(1)(D), added par. (6). Former par. (6) redesignated (7).

Subsec. (b)(6)(B). Pub. L. 108-21, § 508(b)(1)(A), struck out subpar. (B) which read as follows: "if required by section 227 of the Crime Control Act of 1990; or".

Subsec. (b)(7), (8). Pub. L. 108-21, § 508(b)(1)(B), redesignated pars. (6) and (7) as (7) and (8), respectively.

Subsec. (c)(5), (6). Pub. L. 108-21, § 508(b)(2), added par. (5) and redesignated former par. (5) as (6).

2002—Subsec. (b)(5). Pub. L. 107-296, § 225(d)(1)(A), struck out "or" at end.

Subsec. (b)(6)(A). Pub. L. 107-296, § 225(d)(1)(B), inserted "or" at end.

Subsec. (b)(6)(C). Pub. L. 107-296, § 225(d)(1)(C), struck out subpar. (C) which read as follows: "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."

Subsec. (b)(7). Pub. L. 107-296, § 225(d)(1)(D), added par. (7).

2001—Pub. L. 107-56, § 212(a)(1)(A), substituted "Voluntary disclosure of customer communications or records" for "Disclosure of contents" in section catchline.

Subsec. (a)(3). Pub. L. 107-56, § 212(a)(1)(B), added par. (3).

Subsec. (b). Pub. L. 107-56, § 212(a)(1)(C), substituted "Exceptions for disclosure of communications" for "Exceptions" in heading and "A provider described in subsection (a)" for "A person or entity" in introductory provisions.

Subsec. (b)(6)(C). Pub. L. 107-56, § 212(a)(1)(D), added subpar. (C).

Subsec. (c). Pub. L. 107-56, § 212(a)(1)(E), added subsec. (c).

1998—Subsec. (b)(6). Pub. L. 105-314 amended par. (6) generally. Prior to amendment, par. (6) read as follows: "to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime."

1988—Subsec. (b)(2). Pub. L. 100-690 substituted "2517" for "2516".

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

§ 2703. Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to

(B) informs such customer or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1864.)

§ 2706. Cost reimbursement

(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) EXCEPTION.—The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1866; amended Pub. L. 100–690, title VII, § 7061, Nov. 18, 1988, 102 Stat. 4404.)

AMENDMENTS

1988—Subsec. (c). Pub. L. 100–690 inserted heading.

§ 2707. Civil action

(a) CAUSE OF ACTION.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer

or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) IMPROPER DISCLOSURE.—Any willful disclosure of a "record", as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1866; amended Pub. L. 104–293, title VI, § 601(c), Oct. 11, 1996, 110 Stat. 3469; Pub. L. 107–56, title II, §§ 223(b), title VIII, § 815, Oct. 26, 2001, 115 Stat. 293, 384; Pub. L. 107–273, div. B, title IV, § 4005(f)(2), Nov. 2, 2002, 116 Stat. 1813.)

AMENDMENTS

2002—Subsec. (e)(1). Pub. L. 107–273 made technical correction to directory language of Pub. L. 107–56, § 815. See 2001 Amendment note below.

2001—Subsec. (a). Pub. L. 107–56, § 223(b)(1), inserted ", other than the United States," after "person or entity".

Subsec. (d). Pub. L. 107–56, § 223(b)(2), added subsec. (d) and struck out heading and text of former subsec. (d). Text read as follows: "If a court determines that any agency or department of the United States has violated this chapter and the court finds that the circumstances surrounding the violation raise the question whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department concerned shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee."

Subsec. (e)(1). Pub. L. 107–56, § 815, as amended by Pub. L. 107–273, inserted "(including a request of a governmental entity under section 2703(f) of this title after "or a statutory authorization"

Subsec. (g). Pub. L. 107–56, § 223(b)(3), added subsec. (g).

1996—Subsec. (a). Pub. L. 104–293, § 601(c)(1), substituted "other person" for "customer".

Subsec. (c). Pub. L. 104–293, § 601(c)(2), inserted at end "If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court."

Subsecs. (d) to (f). Pub. L. 104–293, § 601(c)(3), (4), added subsec. (d) and redesignated former subsecs. (d) and (e) as (e) and (f), respectively.

EFFECTIVE DATE OF 2002 AMENDMENT

Pub. L. 107–273, div. B, title IV, § 4005(f)(2), Nov. 2, 2002, 116 Stat. 1813, provided that the amendment made by section 4005(f)(2) is effective Oct. 26, 2001.

§ 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1867.)

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may—

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (2015)

drafted by the

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

and by it

APPROVED AND RECOMMENDED FOR ENACTMENT
IN ALL THE STATES

at its

ANNUAL CONFERENCE
MEETING IN ITS ONE-HUNDRED-AND-TWENTY-FOURTH YEAR
WILLIAMSBURG, VIRGINIA
JULY 10 - JULY 16, 2015

WITHOUT PREFATORY NOTE OR COMMENTS

March 8, 2016

REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (2015)

SECTION 1. SHORT TITLE. This [act] may be cited as the Revised Uniform Fiduciary Access to Digital Assets Act (2015).

SECTION 2. DEFINITIONS. In this [act]:

(1) "Account" means an arrangement under a terms-of-service agreement in which a custodian carries, maintains, processes, receives, or stores a digital asset of the user or provides goods or services to the user.

(2) "Agent" means an attorney-in-fact granted authority under a durable or nondurable power of attorney.

(3) "Carries" means engages in the transmission of an electronic communication.

(4) "Catalogue of electronic communications" means information that identifies each person with which a user has had an electronic communication, the time and date of the communication, and the electronic address of the person.

(5) "[Conservator]" means a person appointed by a court to manage the estate of a living individual. The term includes a limited [conservator].

(6) "Content of an electronic communication" means information concerning the substance or meaning of the communication which:

(A) has been sent or received by a user;

(B) is in electronic storage by a custodian providing an electronic-communication service to the public or is carried or maintained by a custodian providing a remote-computing service to the public; and

(C) is not readily accessible to the public.

(7) "Court" means the [insert name of court in this state having jurisdiction in matters

relating to the content of this act].

(8) "Custodian" means a person that carries, maintains, processes, receives, or stores a digital asset of a user.

(9) "Designated recipient" means a person chosen by a user using an online tool to administer digital assets of the user.

(10) "Digital asset" means an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.

(11) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(12) "Electronic communication" has the meaning set forth in 18 U.S.C. Section 2510(12)[, as amended].

(13) "Electronic-communication service" means a custodian that provides to a user the ability to send or receive an electronic communication.

(14) "Fiduciary" means an original, additional, or successor personal representative, [conservator], agent, or trustee.

(15) "Information" means data, text, images, videos, sounds, codes, computer programs, software, databases, or the like.

(16) "Online tool" means an electronic service provided by a custodian that allows the user, in an agreement distinct from the terms-of-service agreement between the custodian and user, to provide directions for disclosure or nondisclosure of digital assets to a third person.

(17) "Person" means an individual, estate, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal

entity.

(18) "Personal representative" means an executor, administrator, special administrator, or person that performs substantially the same function under law of this state other than this [act].

(19) "Power of attorney" means a record that grants an agent authority to act in the place of a principal.

(20) "Principal" means an individual who grants authority to an agent in a power of attorney.

(21) "[Protected person]" means an individual for whom a [conservator] has been appointed. The term includes an individual for whom an application for the appointment of a [conservator] is pending.

(22) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(23) "Remote-computing service" means a custodian that provides to a user computer-processing services or the storage of digital assets by means of an electronic communications system, as defined in 18 U.S.C. Section 2510(14)[, as amended].

(24) "Terms-of-service agreement" means an agreement that controls the relationship between a user and a custodian.

(25) "Trustee" means a fiduciary with legal title to property under an agreement or declaration that creates a beneficial interest in another. The term includes a successor trustee.

(26) "User" means a person that has an account with a custodian.

(27) "Will" includes a codicil, testamentary instrument that only appoints an executor, and instrument that revokes or revises a testamentary instrument.

Legislative Note: In paragraphs (5) and (21), an enacting jurisdiction should replace the bracketed language with local terminology, if different. Enacting jurisdictions should insert the appropriate court in paragraph (7) that would have jurisdiction over matters relating to this act. In jurisdictions in which the constitution, or other law, does not permit the phrase "as amended" when federal statutes are incorporated into state law, the phrase should be deleted in paragraphs (12) and (23).

SECTION 3. APPLICABILITY.

(a) This [act] applies to:

(1) a fiduciary acting under a will or power of attorney executed before, on, or after [the effective date of this [act]];

(2) a personal representative acting for a decedent who died before, on, or after [the effective date of this [act]];

(3) a [conservatorship] proceeding commenced before, on, or after [the effective date of this [act]]; and

(4) a trustee acting under a trust created before, on, or after [the effective date of this [act]].

(b) This [act] applies to a custodian if the user resides in this state or resided in this state at the time of the user's death.

(c) This [act] does not apply to a digital asset of an employer used by an employee in the ordinary course of the employer's business.

Legislative Note: *In subsection (a)(3), an enacting jurisdiction should replace the bracketed language with local terminology, if different.*

SECTION 4. USER DIRECTION FOR DISCLOSURE OF DIGITAL ASSETS.

(a) A user may use an online tool to direct the custodian to disclose to a designated recipient or not to disclose some or all of the user's digital assets, including the content of electronic communications. If the online tool allows the user to modify or delete a direction at

all times, a direction regarding disclosure using an online tool overrides a contrary direction by the user in a will, trust, power of attorney, or other record.

(b) If a user has not used an online tool to give direction under subsection (a) or if the custodian has not provided an online tool, the user may allow or prohibit in a will, trust, power of attorney, or other record, disclosure to a fiduciary of some or all of the user's digital assets, including the content of electronic communications sent or received by the user.

(c) A user's direction under subsection (a) or (b) overrides a contrary provision in a terms-of-service agreement that does not require the user to act affirmatively and distinctly from the user's assent to the terms of service.

SECTION 5. TERMS-OF-SERVICE AGREEMENT.

(a) This [act] does not change or impair a right of a custodian or a user under a terms-of-service agreement to access and use digital assets of the user.

(b) This [act] does not give a fiduciary or designated recipient any new or expanded rights other than those held by the user for whom, or for whose estate, the fiduciary or designated recipient acts or represents.

(c) A fiduciary's or designated recipient's access to digital assets may be modified or eliminated by a user, by federal law, or by a terms-of-service agreement if the user has not provided direction under Section 4.

SECTION 6. PROCEDURE FOR DISCLOSING DIGITAL ASSETS.

(a) When disclosing digital assets of a user under this [act], the custodian may at its sole discretion:

(1) grant a fiduciary or designated recipient full access to the user's account;

(2) grant a fiduciary or designated recipient partial access to the user's account

sufficient to perform the tasks with which the fiduciary or designated recipient is charged: or

(3) provide a fiduciary or designated recipient a copy in a record of any digital asset that, on the date the custodian received the request for disclosure, the user could have accessed if the user were alive and had full capacity and access to the account.

(b) A custodian may assess a reasonable administrative charge for the cost of disclosing digital assets under this [act].

(c) A custodian need not disclose under this [act] a digital asset deleted by a user.

(d) If a user directs or a fiduciary requests a custodian to disclose under this [act] some, but not all, of the user's digital assets, the custodian need not disclose the assets if segregation of the assets would impose an undue burden on the custodian. If the custodian believes the direction or request imposes an undue burden, the custodian or fiduciary may seek an order from the court to disclose:

(1) a subset limited by date of the user's digital assets;

(2) all of the user's digital assets to the fiduciary or designated recipient;

(3) none of the user's digital assets; or

(4) all of the user's digital assets to the court for review in camera.

SECTION 7. DISCLOSURE OF CONTENT OF ELECTRONIC COMMUNICATIONS OF DECEASED USER. If a deceased user consented or a court directs disclosure of the contents of electronic communications of the user, the custodian shall disclose to the personal representative of the estate of the user the content of an electronic communication sent or received by the user if the representative gives the custodian:

(1) a written request for disclosure in physical or electronic form;

(2) a [certified] copy of the death certificate of the user;

(3) a [certified] copy of [the letter of appointment of the representative or a small-estate affidavit or court order];

(4) unless the user provided direction using an online tool, a copy of the user's will, trust, power of attorney, or other record evidencing the user's consent to disclosure of the content of electronic communications; and

(5) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;

(B) evidence linking the account to the user; or

(C) a finding by the court that:

(i) the user had a specific account with the custodian, identifiable by the information specified in subparagraph (A);

(ii) disclosure of the content of electronic communications of the user would not violate 18 U.S.C. Section 2701 et seq.[, as amended], 47 U.S.C. Section 222[, as amended], or other applicable law;

(iii) unless the user provided direction using an online tool, the user consented to disclosure of the content of electronic communications; or

(iv) disclosure of the content of electronic communications of the user is reasonably necessary for administration of the estate.

Legislative Note: *In jurisdictions that certify legal documents, the word "certified" should be included in paragraphs (2) and (3). Other jurisdictions may substitute a word or phrase that conforms to the local practice for authentication. Enacting jurisdictions should insert into paragraph (3) the local term given to a document that authorizes a personal representative to administer a decedent's estate. In jurisdictions in which the constitution, or other law, does not permit the phrase "as amended" when federal statutes are incorporated into state law, the phrase should be deleted in paragraph (5)(C)(ii).*

SECTION 8. DISCLOSURE OF OTHER DIGITAL ASSETS OF DECEASED USER. Unless the user prohibited disclosure of digital assets or the court directs otherwise, a custodian shall disclose to the personal representative of the estate of a deceased user a catalogue of electronic communications sent or received by the user and digital assets, other than the content of electronic communications, of the user, if the representative gives the custodian:

(1) a written request for disclosure in physical or electronic form;

(2) a [certified] copy of the death certificate of the user;

(3) a [certified] copy of [the letter of appointment of the representative or a small-estate affidavit or court order]; and

(4) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;

(B) evidence linking the account to the user;

(C) an affidavit stating that disclosure of the user's digital assets is reasonably necessary for administration of the estate; or

(D) a finding by the court that:

(i) the user had a specific account with the custodian, identifiable by the information specified in subparagraph (A); or

(ii) disclosure of the user's digital assets is reasonably necessary for administration of the estate.

Legislative Note: *In jurisdictions that certify legal documents, the word "certified" should be included in paragraphs (2) and (3). Other jurisdictions may substitute a word or phrase that conforms to the local practice for authentication. Enacting jurisdictions should insert into paragraph (3) the local term given to a document that authorizes a personal representative to administer a decedent's estate.*

SECTION 9. DISCLOSURE OF CONTENT OF ELECTRONIC COMMUNICATIONS OF PRINCIPAL. To the extent a power of attorney expressly grants an agent authority over the content of electronic communications sent or received by the principal and unless directed otherwise by the principal or the court, a custodian shall disclose to the agent the content if the agent gives the custodian:

(1) a written request for disclosure in physical or electronic form;

(2) an original or copy of the power of attorney expressly granting the agent authority over the content of electronic communications of the principal;

(3) a certification by the agent, under penalty of perjury, that the power of attorney is in effect; and

(4) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the principal's account; or

(B) evidence linking the account to the principal.

SECTION 10. DISCLOSURE OF OTHER DIGITAL ASSETS OF PRINCIPAL. Unless otherwise ordered by the court, directed by the principal, or provided by a power of attorney, a custodian shall disclose to an agent with specific authority over digital assets or general authority to act on behalf of a principal a catalogue of electronic communications sent or received by the principal and digital assets, other than the content of electronic communications, of the principal if the agent gives the custodian:

(1) a written request for disclosure in physical or electronic form;

(2) an original or a copy of the power of attorney that gives the agent specific authority over digital assets or general authority to act on behalf of the principal;

(3) a certification by the agent, under penalty of perjury, that the power of attorney is in effect: and

(4) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the principal's account; or

(B) evidence linking the account to the principal.

SECTION 11. DISCLOSURE OF DIGITAL ASSETS HELD IN TRUST WHEN TRUSTEE IS ORIGINAL USER. Unless otherwise ordered by the court or provided in a trust, a custodian shall disclose to a trustee that is an original user of an account any digital asset of the account held in trust, including a catalogue of electronic communications of the trustee and the content of electronic communications.

SECTION 12. DISCLOSURE OF CONTENTS OF ELECTRONIC COMMUNICATIONS HELD IN TRUST WHEN TRUSTEE NOT ORIGINAL USER. Unless otherwise ordered by the court, directed by the user, or provided in a trust, a custodian shall disclose to a trustee that is not an original user of an account the content of an electronic communication sent or received by an original or successor user and carried, maintained, processed, received, or stored by the custodian in the account of the trust if the trustee gives the custodian:

(1) a written request for disclosure in physical or electronic form;

(2) a certified copy of the trust instrument[or a certification of the trust under [cite trust-certification statute, such as Uniform Trust Code Section 1013]] that includes consent to disclosure of the content of electronic communications to the trustee;

(3) a certification by the trustee, under penalty of perjury, that the trust exists and the

trustee is a currently acting trustee of the trust; and

(4) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the trust's account; or

(B) evidence linking the account to the trust.

SECTION 13. DISCLOSURE OF OTHER DIGITAL ASSETS HELD IN TRUST WHEN TRUSTEE NOT ORIGINAL USER. Unless otherwise ordered by the court, directed by the user, or provided in a trust, a custodian shall disclose, to a trustee that is not an original user of an account, a catalogue of electronic communications sent or received by an original or successor user and stored, carried, or maintained by the custodian in an account of the trust and any digital assets, other than the content of electronic communications, in which the trust has a right or interest if the trustee gives the custodian:

(1) a written request for disclosure in physical or electronic form;

(2) a certified copy of the trust instrument[or a certification of the trust under [cite trust-certification statute, such as Uniform Trust Code Section 1013]];

(3) a certification by the trustee, under penalty of perjury, that the trust exists and the trustee is a currently acting trustee of the trust; and

(4) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the trust's account; or

(B) evidence linking the account to the trust.

SECTION 14. DISCLOSURE OF DIGITAL ASSETS TO [CONSERVATOR] OF [PROTECTED PERSON].

(a) After an opportunity for a hearing under [state conservatorship law], the court may grant a [conservator] access to the digital assets of a [protected person].

(b) Unless otherwise ordered by the court or directed by the user, a custodian shall disclose to a [conservator] the catalogue of electronic communications sent or received by a [protected person] and any digital assets, other than the content of electronic communications, in which the [protected person] has a right or interest if the [conservator] gives the custodian:

(1) a written request for disclosure in physical or electronic form;

(2) a [certified] copy of the court order that gives the [conservator] authority over the digital assets of the [protected person]; and

(3) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the account of the [protected person]; or

(B) evidence linking the account to the [protected person].

(c) A [conservator] with general authority to manage the assets of a [protected person] may request a custodian of the digital assets of the [protected person] to suspend or terminate an account of the [protected person] for good cause. A request made under this section must be accompanied by a [certified] copy of the court order giving the [conservator] authority over the protected person's property.

Legislative Note: *Throughout this section, an enacting jurisdiction should replace the bracketed terms [conservator] and [protected person] with local terminology, if different. In jurisdictions that certify legal documents, the word "certified" should be included in subsections (b) and (c). Other jurisdictions may substitute a word or phrase that conforms to the local practice for authentication.*

SECTION 15. FIDUCIARY DUTY AND AUTHORITY.

(a) The legal duties imposed on a fiduciary charged with managing tangible property apply to the management of digital assets, including:

(1) the duty of care;

(2) the duty of loyalty; and

(3) the duty of confidentiality.

(b) A fiduciary's or designated recipient's authority with respect to a digital asset of a user:

(1) except as otherwise provided in Section 4, is subject to the applicable terms of service;

(2) is subject to other applicable law, including copyright law;

(3) in the case of a fiduciary, is limited by the scope of the fiduciary's duties; and

(4) may not be used to impersonate the user.

(c) A fiduciary with authority over the property of a decedent, [protected person], principal, or settlor has the right to access any digital asset in which the decedent, [protected person], principal, or settlor had a right or interest and that is not held by a custodian or subject to a terms-of-service agreement.

(d) A fiduciary acting within the scope of the fiduciary's duties is an authorized user of the property of the decedent, [protected person], principal, or settlor for the purpose of applicable computer-fraud and unauthorized-computer-access laws, including [this state's law on unauthorized computer access].

(e) A fiduciary with authority over the tangible, personal property of a decedent, [protected person], principal, or settlor:

(1) has the right to access the property and any digital asset stored in it; and

(2) is an authorized user for the purpose of computer-fraud and unauthorized-computer-access laws, including [this state's law on unauthorized computer access].

(f) A custodian may disclose information in an account to a fiduciary of the user when the information is required to terminate an account used to access digital assets licensed to the user.

(g) A fiduciary of a user may request a custodian to terminate the user's account. A request for termination must be in writing, in either physical or electronic form, and accompanied by:

(1) if the user is deceased, a [certified] copy of the death certificate of the user;

(2) a [certified] copy of the [letter of appointment of the representative or a small-estate affidavit or court order,] court order, power of attorney, or trust giving the fiduciary authority over the account; and

(3) if requested by the custodian:

(A) a number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;

(B) evidence linking the account to the user; or

(C) a finding by the court that the user had a specific account with the custodian, identifiable by the information specified in subparagraph (A).

Legislative Note: *States with a computer trespass statute should cite to it in subsections (d) and (e), and may want to amend those statutes to be in accord with this act. In jurisdictions that certify legal documents, the word "certified" should be included in subsection (g). Other jurisdictions may substitute a word or phrase that conforms to the local practice for authentication. In subsections (c) and (e), an enacting jurisdiction should replace the bracketed language with local terminology, if different.*

SECTION 16. CUSTODIAN COMPLIANCE AND IMMUNITY.

(a) Not later than [60] days after receipt of the information required under Sections 7 through 15, a custodian shall comply with a request under this [act] from a fiduciary or designated recipient to disclose digital assets or terminate an account. If the custodian fails to comply, the fiduciary or designated recipient may apply to the court for an order directing compliance.

(b) An order under subsection (a) directing compliance must contain a finding that compliance is not in violation of 18 U.S.C. Section 2702[, as amended].

(c) A custodian may notify the user that a request for disclosure or to terminate an account was made under this [act].

(d) A custodian may deny a request under this [act] from a fiduciary or designated recipient for disclosure of digital assets or to terminate an account if the custodian is aware of any lawful access to the account following the receipt of the fiduciary's request.

(e) This [act] does not limit a custodian's ability to obtain or require a fiduciary or designated recipient requesting disclosure or termination under this [act] to obtain a court order which:

(1) specifies that an account belongs to the [protected person] or principal;

(2) specifies that there is sufficient consent from the [protected person] or principal] to support the requested disclosure; and

(3) contains a finding required by law other than this [act].

(f) A custodian and its officers, employees, and agents are immune from liability for an act or omission done in good faith in compliance with this [act].

Legislative Note: *In jurisdictions in which the constitution, or other law, does not permit the phrase "as amended" when federal statutes are incorporated into state law, the phrase should be deleted in subsection (b). In subsection (e), an enacting jurisdiction should replace the bracketed language with local terminology, if different.*

SECTION 17. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

SECTION 18. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. This [act] modifies, limits, or supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 et seq., but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

[SECTION 19. SEVERABILITY. If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.]

Legislative Note: *Include this section only if the jurisdiction lacks a general severability statute or a decision by the highest court of the jurisdiction stating a general rule of severability.*

SECTION 20. REPEALS; CONFORMING AMENDMENTS.

(a) ....

(b) ....

(c) ....

SECTION 21. EFFECTIVE DATE. This [act] takes effect....