Law and Policy at the Bleeding Edge: 2016 Technology Law Updates

Cosponsored by the Technology Law Section

Friday, October 14, 2016
8:50 a.m.–5 p.m.

6.75 General CLE credits
The materials and forms in this manual are published by the Oregon State Bar exclusively for the use of attorneys. Neither the Oregon State Bar nor the contributors make either express or implied warranties in regard to the use of the materials and/or forms. Each attorney must depend on his or her own knowledge of the law and expertise in the use or modification of these materials.

Copyright © 2016

OREGON STATE BAR
16037 SW Upper Boones Ferry Road
P.O. Box 231935
Tigard, OR 97281-1935
# TABLE OF CONTENTS

## Schedule

| Schedule | v |

## Faculty

| Faculty | vii |

## 1. War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property |

- Victoria Blachly, *Samuels Yoelin Kantor, Portland, Oregon*

## 2. Technology and Agriculture: Emerging Trends and Legal Issues—Presentation Slides |

- Mary Anne Nash, *Oregon Farm Bureau, Salem, Oregon*
- Jennifer Dresler, *Oregon Farm Bureau, Salem, Oregon*

## 3. Drone Law: Updates and Guidance—Presentation Slides |

- Craig Russillo, *Schwabe Williamson & Wyatt, Portland, Oregon*

## 4. Oregon Energy and Climate Policy—Presentation Slides |

- Kristin Eberhard, *Sightline Institute, Portland, Oregon*

## 5. Stingray Technology and Associated Legal Issues—Presentation Slides |

- Professor Carrie Leonetti, *University of Oregon School of Law, Portland, Oregon*

## 6. Connecting to Our Future: The Digital Livable City |

- Mary Beth Henry, *Portland, Oregon*
- David Olson, *Cableworks, Portland, Oregon*

## 7. Self-Driving Vehicle Technology, Policy, and Liability—Presentation Slides |

- Richard Lazar, *Techolicy, Portland, Oregon*
- Josh Schoonmaker, *Director of Business Development, Tozny, Portland, Oregon*
SCHEDULE

8:00 Registration

8:50 Opening Remarks

9:00 Drone Law: Updates and Guidance
   ♦ New FAA rules for commercial use of small drones
   ♦ Privacy concerns
   ♦ Liability and insurance considerations
   Craig Russillo, Schwabe Williamson & Wyatt, Portland

10:00 Technology and Agriculture: Emerging Trends and Legal Issues
   ♦ How drones and biotechnology are expanding agricultural frontiers
   ♦ Advising clients in a changing federal and state regulatory landscape
   Jennifer Dresler, Oregon Farm Bureau, Salem
   Mary Anne Nash, Oregon Farm Bureau, Salem

11:00 Break

11:15 War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property
   ♦ What happens to digital legacies after death?
   ♦ How to be proactive under the Revised Uniform Financial Access to Digital Assets Act (RUFADAA)
   ♦ Strategies for effective digital asset management
   Victoria Blachly, Samuels Yoelin Kantor, Portland

12:15 Break

12:30 Lunch Presentation: Oregon Energy and Climate Policy
   ♦ Carbon pricing globally and in Oregon
   ♦ Oregon’s transportation package and climate issues
   ♦ Washington’s policies and programs
   Kristin Eberhard, Sightline Institute, Portland

1:30 Stingray Technology and Associated Legal Issues
   ♦ Fourth Amendment and probable cause
   ♦ Constitutional significance of inadvertently intercepted data
   ♦ Stingray technology secrecy and constitutional implications
   Professor Carrie Leonetti, University of Oregon School of Law, Portland

2:30 Break

2:45 Connecting to Our Future: The Digital Livable City
   ♦ Avoiding the “digital divide”
   ♦ Creating livable cities and combatting climate change
   ♦ Legal, administrative, and political challenges in technological planning
   David Olson, Adjunct Professor, Telecommunications Law, Lewis & Clark Law School, Portland
3:45  Self-Driving Vehicles—Technology, Policy, and Liability Issues

- The speed of autonomous vehicle evolution
- How autonomous vehicles impact our lives
- Autonomous vehicle public policy, legal, and liability issues

Richard Lazar, Techolicy, Portland
Josh Schoonmaker, Director of Business Development, Tozny, Portland

5:00  Adjourn
Victoria Blachly, Samuels Yoelin Kantor, Portland. Ms. Blachly is a fiduciary litigator who represents individual trustees, corporate trustees, beneficiaries, and personal representatives in cases including trust and estate litigation, will contests, trust disputes, undue influence, capacity, claims of fiduciary breach, financial elder abuse, petitioning for court instructions, and contested guardianship and conservatorship. She is engaged in state and national lobbying for updating laws for fiduciaries, and she serves as a commissioner to the Governor’s Commission on Senior Services. Ms. Blachly writes for and lectures at national and state legal seminars pertaining to trusts and estates, and she is a frequent law blogger for Samuels Yoelin Kantor’s wealthlawblog.com.

Jennifer Dresler, Oregon Farm Bureau, Salem. Ms. Dresler serves as Director of State Public Policy for the Oregon Farm Bureau, the state’s largest farm and ranch membership organization, where her extensive science background informs public policy work at the capitol and with state agencies. She also coordinates grassroots and campaign efforts for the Oregon Farm Bureau. Previously, Ms. Dresler worked for Oregon State Senator Ted Ferrioli in both his legislative and campaign operations and as a policy analyst for the Oregon Senate Republican Office, and before that she was a Knauss Legislative Fellow in the office of U.S. Senator Roger Wicker (R–MS) in Washington, D.C., focusing on policy research related to science, economic development, and transportation infrastructure. She holds a Masters in Environmental Science from Oregon State University.

Kristin Eberhard, Sightline Institute, Portland. Ms. Eberhard researches, writes about, and speaks about climate change policy and democracy reform. Before joining Sightline, Ms. Eberhard worked at the Natural Resources Defense Council, where she led its California climate work in San Francisco and the moved to its Southern California office to help the largest municipally owned utility in the country get off coal and onto energy efficiency and renewables. She also taught courses on climate change and energy law at Stanford Law School and UCLA School of Law. She holds a Masters of Environmental Management from the Duke University Nicholas School of the Environment.

Richard Lazar, Techolicy, Portland.

Professor Carrie Leonetti, University of Oregon School of Law, Portland. Professor Leonetti is an Associate Professor of Constitutional Law, Criminal Procedure, and Evidence and the Faculty Leader of the Criminal Justice Initiative at the University of Oregon School of Law in Portland. She teaches classes in constitutional law, criminal procedure, trial practice, mental health, and forensic science. She is also the faculty supervisor for Criminal Practice Externships at U of O. Her scholarship focuses on constitutional criminal procedure, high-tech surveillance, prosecutorial discretion, the effectiveness of defense counsel, and comparative criminal procedure. Professor Leonetti previously was an Assistant Federal Defender in the Eastern District of California, an Assistant Public Defender in the Appellate Division of the Office of the Maryland Public Defender, and a member of the ABA Criminal-Justice Standards DNA Task Force.

Mary Anne Nash, Oregon Farm Bureau, Salem. Ms. Nash is the Public Policy Counsel and Director of Regulatory Affairs at the Oregon Farm Bureau. In addition to representing the Oregon Farm Bureau on legal issues, she works with state and federal agencies on water quality, water supply, removal-fill, Endangered Species Act, NEPA, land use, acquisition, and other natural resources issues. Prior to her current position, Ms. Nash was in private practice in Portland, representing agricultural producers on a wide variety of federal and state issues. Ms. Nash is chair-elect of the Oregon State Bar Agricultural Law Section.
David Olson, Adjunct Professor, Telecommunications Law, Lewis & Clark Law School, Portland. Professor Olson served for nearly 30 years as Cable Director for the City of Portland, where he oversaw Portland’s cable, telecommunications, and utility franchise programs and served as staff director for the Mt. Hood Cable Regulatory Commission. He stepped down as Portland’s Cable Director in 2012 to concentrate on teaching and consulting projects. He serves as Adjunct Professor at Lewis and Clark Law School, where he teaches Telecommunications Law. He also teaches online at DeVry University and maintains an active consulting practice (Cableworks) in his field of telecommunications law and regulation. Professor Olson is a member of the Federal Communications Bar Association and past president of the National Association of Telecommunications Officers and Advisors.

Craig Russillo, Schwabe Williamson & Wyatt, Portland. Mr. Rusillo works extensively with lenders and creditors in judicial and nonjudicial foreclosures, representing their interests in state, federal, and bankruptcy courts. He also has significant experience with real property disputes, including complex title issues, landlord/tenant disputes, and construction matters. In addition, Mr. Rusillo heads Schwabe’s team representing clients in the burgeoning field of unmanned aerial vehicles (drones). He is a frequent speaker to industry clients and trade groups regarding the current state and federal regulations applicable to the commercial use of drones, and he represents clients before the Federal Aviation Administration seeking authority for the commercial use of drones. Mr. Rusillo is a member of the Association of Unmanned Vehicles International, the leading trade organization for the drone industry. He is admitted to practice in Oregon and Washington.

Josh Schoonmaker, Director of Business Development, Tozny, Portland. Mr. Schoonmaker is the head of business development for Tozny, a Portland-based data privacy and authentication startup. He is a technology company veteran who has worked on innovation initiatives for HP, Disney, eBay, and PayPal. He is the author of “Proactive Privacy for a Driverless Age,” Journal of Information & Communications Technology Law, which focuses on autonomous vehicle data privacy. Mr. Schoonmaker holds MBA and Master of Legal Studies degrees from Willamette University.
# War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

**Victoria Blachly**  
Samuels Yoelin Kantor  
Portland, Oregon

## Contents

<table>
<thead>
<tr>
<th>Terms of Service for Selected Internet Accounts</th>
<th>1–1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>iCloud</strong></td>
<td>1–1</td>
</tr>
<tr>
<td>2. <strong>Yahoo</strong></td>
<td>1–1</td>
</tr>
<tr>
<td>3. <strong>Google</strong></td>
<td>1–1</td>
</tr>
<tr>
<td>4. <strong>Microsoft</strong></td>
<td>1–2</td>
</tr>
<tr>
<td>5. <strong>Facebook</strong></td>
<td>1–5</td>
</tr>
<tr>
<td>Estate Planning Provisions—Fiduciary Authorization Examples</td>
<td>1–6</td>
</tr>
<tr>
<td>Virtual Asset Instruction Letters</td>
<td>1–9</td>
</tr>
<tr>
<td>Revised UFADDA Summary</td>
<td>1–13</td>
</tr>
<tr>
<td>Oregon Senate Bill 1554</td>
<td>1–15</td>
</tr>
<tr>
<td>Revised UFADAA with Commentary (2015)</td>
<td>1–23</td>
</tr>
<tr>
<td>Google Letter</td>
<td>1–59</td>
</tr>
<tr>
<td>Facebook Letter</td>
<td>1–61</td>
</tr>
<tr>
<td>Revised UFADAA Comparison with PEAC Act</td>
<td>1–63</td>
</tr>
<tr>
<td>“Uniform Fiduciary Access to Digital Assets Act: What UFADAA Know”</td>
<td>1–65</td>
</tr>
<tr>
<td>“Planning for Fiduciary Access to Digital Assets”</td>
<td>1–85</td>
</tr>
<tr>
<td>Presentation Slides</td>
<td>1–93</td>
</tr>
</tbody>
</table>
Terms of Service for Selected Internet Accounts

1. iCloud

No Right of Survivorship
You agree that your Account is non-transferable and that any rights to your Apple ID or Content within your Account terminate upon your death. Upon receipt of a copy of a death certificate your Account may be terminated and all Content within your Account deleted. Contact iCloud Support at www.apple.com/support/icloud for further assistance.


2. Yahoo!

No Right of Survivorship and Non-Transferability. You agree that your Yahoo account is non-transferable and any rights to your Yahoo ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.


3. Google

Submit a request regarding a deceased user's account
Users have a strong and reasonable expectation of privacy and security when using Google’s products. We believe that the trust placed in us by our users requires us to make sure that their information is safe, even in the event of their death.

Inactive Account Manager is the best way for you to let us know who should have access to your information, and whether you want your account to be deleted. Click here to set up Inactive Account Manager for your account.

We recognize, however, that many people pass away without leaving clear instructions about how to manage their online accounts. We can work with immediate family members and representatives to close online accounts in some cases once a user is known to be deceased, and in certain circumstances we may provide content from a deceased user’s account. In all of these cases, our primary responsibility is to keep our users’ information secure, safe, and private. Note that Google is not able to provide passwords or other mechanisms that would enable anyone to log in to a user’s account.
Before you begin, please understand that sending a request or filing the required documentation does not guarantee that Google will be able to assist you. Any decision to satisfy a request about a deceased user will be made only after a careful review.

**Google Inactive Account Manager**

What should happen to your photos, emails and documents when you stop using your account? Google puts you in control.

You might want your data to be shared with a trusted friend or family member, or, you might want your account to be deleted entirely. There are many situations that might prevent you from accessing or using your Google account. Whatever the reason, we give you the option of deciding what happens to your data.

Using Inactive Account Manager, you can decide if and when your account is treated as inactive, what happens with your data and who is notified.

**Timeout period**

You set a timeout period, after which your account can be treated as inactive. The timeout period starts with your last sign-in to your Google account.

**Alert me**

Inactive Account Manager will alert you via text message and optionally email before the timeout period ends.

**Notify contacts and share data**

Add trusted contacts who should be made aware that you are no longer using your account. You can also share data with them if you like.

**Optionally delete account**

If you wish, instruct Google to delete your account on your behalf.

Source: https://support.google.com/accounts/contact/deceased?rd=1

4. Microsoft

Microsoft Next of Kin Process: What to do in the event of the death or incapacitation of a loved one with a Outlook.com account.
If you have lost a family member, or have a family member who has become medically incapacitated, the following information will help you contact Microsoft regarding their Outlook.com account.

**What can Microsoft provide me with in relation to my family member’s Outlook.com account?**

The Microsoft Next of Kin process allows for the release of Outlook.com contents, including all emails and their attachments, address book, and Messenger contact list, to the next of kin of a deceased or incapacitated account holder and/or closure of the Microsoft account, following a short authentication process. We cannot provide you with the password to the account or change the password on the account, and we cannot transfer ownership of the account to the next of kin. Account contents are released by way of a data DVD which is shipped to you. Unfortunately, the Next of Kin department cannot assist you with password resets, account recovery, or any other support for your own account.

**What products does the Microsoft Next of Kin process support?**

At this time, the Microsoft Next of Kin process supports only Outlook.com accounts (email accounts ending in @outlook.com, @hotmail.com, @live.com, @windowslive.com, or @msn.com). We do not provide support for SkyDrive, MSN Dial-up, or Xbox Live.

**How do I request the contents of my family member’s account, or request the closure of the account?**

In order to request that the contents of the email account be released to you, or to request the closure of the account, please contact the Microsoft Custodian of Records by emailing msrecord@microsoft.com to initiate the process. To process your request, we require that you provide some information about the account as well as copies of documentation to verify the status of the account holder and your kinship. Please refer to “What information and documentation will I need to provide for the next of kin process?” Please also provide us with an email address where we can reach you in case we have any follow-up questions and so we can notify you of the status of your request.

**What documentation will I need to provide for the next of kin process?**

In order to prove that you are legal next of kin and that the account holder is deceased or incapacitated, we require the following documentation:

1) An official death certificate for the user, if the user is deceased. Unfortunately, we cannot accept anything other than an official, government issued death certificate. Examples of documents which we cannot accept are:
a. An obituary
b. A coroner’s interim death certificate
c. A coroner’s statement of inquest into a death
d. A funeral director’s statement of services performed

2) A certified document signed by a medical professional in charge of the care of the user, if the user is incapacitated. A note signed by the doctor in charge and notarized will suffice, as will a signed court document showing that you have power of attorney or executorship of a trust for the account holder.

3) A Document showing that you are the user’s next of kin and/or executor or benefactor of their estate, or that you have power of attorney. We accept any of the following documents as proof of kinship or executor status:
   a. A marriage certificate showing that you are the surviving spouse of the account holder.
   b. Signed power of attorney paperwork.
   c. A copy of a will or trust document naming you as executor or beneficiary.
   d. A birth certificate for the user, if you are their parent; or guardianship paperwork for legal guardians.

4) A photocopy of your government issued photo ID.

What information will I need to know about the Outlook.com account?

We require answers to all of the following questions about the account holder’s email account.

1) What is or are the email address or addresses?
2) What is the first and last name that the account holder used when creating the account?
3) What is the date of birth that the account holder gave when creating the account?
4) What city, state, and zip code (for U.S. users) or country did the account holder enter as their place of residence when the account was created?
5) Approximately when was the account created? This doesn’t need to be anything specific. “During the late 1990s,” or “Around 2004” are perfectly acceptable answers.
6) Approximately when was the account last accessed? It is important that you tell us if you have been checking the account past the account holder’s date of death, or if you suspect that the account has been accessed by an unauthorized individual after the account holder’s death.
7) Your shipping address, if you are requesting a copy of the contents of the account.

Please note that we cannot ship to a P.O. Box. Since your shipment will be coming from the U.S., please include your shipping address in the following format:
   a. Attention
   b. Street Address
   c. City
   d. State/Province
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

8) What type of computer you use, if you are requesting a copy of the contents of the account. We support PC, Mac, and Linux users, but we need to know what type of computer you use for preservation purposes.


5. Facebook

How do I report a deceased person or an account that needs to be memorialized?

Memorializing the account:
We will memorialize the Facebook account of a deceased person when we receive a valid request.
We try to prevent references to memorialized accounts from appearing on Facebook in ways that may be upsetting to the person's friends and family, and we also take measures to protect the privacy of the deceased person by securing the account.
Please keep in mind that we cannot provide login information for a memorialized account. It is always a violation of our policies to log into another person's account.
To report a profile to be memorialized, please contact us.

Removing the account:
Verified immediate family members may request the removal of a loved one’s account from Facebook.

Source: https://www.facebook.com/help/150486848354038

What's the difference between deactivating and deleting my account?
You can deactivate or delete your account at any time.
You may deactivate your account for any number of temporary reasons. This option gives you the flexibility to leave and come back whenever you want. If you deactivate your account:
People won’t be able to see the information on your Timeline on Facebook.
People on Facebook will not be able to search for you.
Some information, like messages you sent, may still be visible to others.
We save the information in your account (ex: friends, photos, interests), just in case you want to come back to Facebook at some point. If you choose to reactivate your account, the information on your profile will be there when you come back.
If you permanently delete your account:
You will not be able to regain access to your account.
Some of the things you do on Facebook aren’t stored in your account. For example, a friend may still have messages from you even after you delete your account. That information remains after you delete your account.

It may take up to 90 days to delete all of the things you've posted, like your photos, status updates or other data stored in backup systems. While we are deleting this information, it is inaccessible to other people using Facebook.

Copies of some material (ex: log records) may remain in our database for technical reasons. When you delete your account, this material is disassociated from any personal identifiers.

Source: https://www.facebook.com/help/125338004213029

Estate Planning Provisions – Fiduciary Authorizations:

Provision for Power of Attorney

Specific Powers. Without in any way limiting the generality of the power and authority conferred upon my agent under Section 1, my agent shall have and may exercise the specific powers set forth below.

(xxx) Digital Assets. To access, modify, control, archive, transfer, and delete my digital assets. Digital assets include my sent and received emails, email accounts, digital music, digital photographs, digital videos, gaming accounts, software licenses, social-network accounts, file-sharing accounts, financial accounts, domain registrations, Domain Name System (DNS) service accounts, blogs, listservs, web-hosting accounts, tax-preparation service accounts, online stores and auction sites, online accounts, and any similar digital asset that currently exists or may be developed as technology advances. My digital assets may be stored on the cloud or on my own digital devices. My agent may access, use, and control my digital devices in order to access, modify, control, archive, transfer, and delete my digital assets—this power is essential for access to my digital assets that are only accessible through my digital devices. Digital devices include desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smartphones, and any similar hardware that currently exists or may be developed as technology advances.

A More Comprehensive Provision

The powers of my Personal Representative and the Trustee shall also include the following powers:
Digital Assets and Accounts. My Personal Representative or the Trustee may take any action (including, without limitation, changing a terms of service agreement or other governing instrument) with respect to my Digital Assets and Digital Accounts as my Personal Representative or the Trustee shall deem appropriate, and as shall be permitted under applicable state and Federal law. My Personal Representative or the Trustee may engage experts or consultants or any other third party, and may delegate authority to such experts, consultants or third party, as necessary or appropriate to effectuate such actions with respect to my Digital Assets or Digital Accounts, including, but not limited to, such authority as may be necessary or appropriate to decrypt electronically stored information, or to bypass, reset or recover any password or other kind of authentication or authorization. If my Personal Representative or the Trustee shall determine that it is necessary or appropriate to engage and delegate authority to an individual pursuant to this paragraph, it is my request that [Insert Name of Digital Asset Representative] be engaged for this purpose. This authority is intended to constitute "lawful consent" to a service provider to divulge the contents of any communication under The Stored Communications Act (currently codified as 18 U.S.C. §§ 2701 et seq.), to the extent such lawful consent is required, and a Personal Representative or Trustee acting hereunder shall be an authorized user for purposes of applicable computer-fraud and unauthorized-computer-access laws. The authority granted under this paragraph shall extend to all Digital Assets and Digital Accounts associated with or used in connection with the Business (as defined in the Article herein entitled "The Closely-Held Business"). The authority granted under this paragraph is intended to provide my Personal Representative or the Trustee with full authority to access and manage my Digital Assets and Digital Accounts, to the extent permitted under applicable state and Federal law and shall not limit any authority granted to my Personal Representative or the Trustee under such laws.

The following definitions and miscellaneous provisions shall apply under this Will:

Digital Assets, Accounts and Devices. The following definitions and descriptions shall apply to the authority of the Personal Representative and Trustee with respect to my Digital Assets and Accounts:

“Digital Assets” shall include files created, generated, sent, communicated, shared, received, or stored on a Digital Device, regardless of the ownership of the physical device upon which the digital item was created, generated, sent, communicated, shared, received or stored (which underlying physical device shall not be a "Digital Asset" for purposes of this Will)

A "Digital Device" is an electronic device that can create, generate, send, share, communicate, receive, store, display, or process information, including, without limitation, desktops, laptops, tablets, peripherals, storage, devices, mobile telephones, smart phones, cameras, electronic reading devices and any similar digital device which currently exists or may exist as technology develops or such comparable items as technology develops.
"Digital Account" means an electronic system for creating, generating, sending, sharing, communicating, receiving, storing, displaying, or processing information which provides access to a Digital Asset stored on a Digital Device, regardless of the ownership of such Digital Device.

For the purpose of illustration, and without limitation, Digital Assets and Digital Accounts shall include email and email accounts, social network content and accounts, social media content and accounts, text, documents, digital photographs, digital videos, software, software licenses, computer programs, computer source codes, databases file sharing accounts, financial accounts, health insurance records and accounts, health care records and accounts, domain registrations, DNS service accounts, web hosting accounts, tax preparation service accounts, online store accounts and affiliate programs and other online accounts which currently exist or may exist as technology develops, or such comparable items and accounts as technology develops, including any words, characters, codes, or contractual rights necessary to access such items and accounts.
VIRTUAL ASSET INSTRUCTION LETTERS

The steps that we recommend for a Virtual Asset Instruction Letter (“VAIL”):

• First, identify each internet account that you have and determine how each company handles an account when the account holder dies.

• Second, determine which accounts you want your representative to maintain and have access to, and prepare a written and electronic file list of those accounts with their passwords.

• Third, determine which accounts you wish to have deleted and provide the necessary written instructions to do so.

• Fourth, consider saving the account and access information on a CD or memory stick and store it in a safe place. Give your representative instructions about how to access this information. Don’t forget to update it as passwords change.

• Fifth, if you have a collection of pictures or other memorabilia that are being stored on the internet, consider making a backup of that information to a disk drive or CD that you control. Store this information in a safe place, and provide your personal representative with instructions on how to obtain that information.

• Sixth, upgrade your power of attorney to include provisions authorizing your agent to access your emails and other electronic data.

• Seventh, if someone other than your personal representative is being designated to handle your electronic data, then those individuals should be named in your will or other estate planning documents.

For more detailed information go to www.wealthlawblog.com
WHY YOUR STATE SHOULD ADOPT THE
REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (2015)

The Revised Uniform Fiduciary Access to Digital Assets Act (Revised UFADAA) modernizes fiduciary law for the Internet age. Fiduciaries are the people appointed to manage our property when we die or lose the capacity to manage it ourselves. Nearly everyone today has digital assets, such as documents, photographs, email, and social media accounts, and fiduciaries are often prevented from accessing those accounts by password protection or restrictive terms of service. Digital assets may have real value, both monetary and sentimental, but they also present novel privacy concerns. UFADAA provides legal authority for fiduciaries to manage digital assets in accordance with the user’s estate plan, while protecting a user’s private communications from unwarranted disclosure.

- **Revised UFADAA gives Internet users control.** Revised UFADAA allows users to specify whether their digital assets should be preserved, distributed to heirs, or destroyed.

- **Revised UFADAA provides efficient uniformity for all concerned.** Digital assets travel across state lines nearly instantaneously. In our modern mobile society, people relocate more often than ever. Because state law governs fiduciaries, a uniform law ensures that fiduciaries in every state will have equal access to digital assets and custodians will have a single legal standard with which to comply.

- **Revised UFADAA respects privacy interests.** Private communications like email and social media conversations are protected by federal privacy law. Revised UFADAA prevents the companies that store our communications from releasing them to fiduciaries unless the user consented to disclosure.

- **Revised UFADAA addresses four common types of fiduciaries.** Revised UFADAA provides appropriate default rules governing access to digital assets for executors of a decedent’s estate, agents under a power of attorney, conservators, and trustees.

- **Revised UFADAA works hand-in-hand with federal and state law.** Under Revised UFADAA, fiduciaries must provide proof of their authority in the form of a certified document. Custodians of digital assets that comply with a fiduciary’s apparently authorized request for access are immune from any liability under statutes that prohibit unauthorized access. A fiduciary’s authority over digital assets is limited by federal law, including the Copyright Act and the Electronic Communications Privacy Act.

For further information about Revised UFADAA, please contact ULC Legislative Counsel Benjamin Orzeske at 312-450-6621 or borzeske@uniformlaws.org.

The ULC is a nonprofit formed in 1892 to create nonpartisan state legislation. Over 350 volunteer commissioners—lawyers, judges, law professors, legislative staff, and others—work together to draft laws ranging from the Uniform Commercial Code to acts on property, trusts and estates, family law, criminal law and other areas where uniformity of state law is desirable.
In the Internet age, the nature of property and our methods of communication have changed dramatically. A generation ago, a human being delivered our mail, photos were kept in albums, documents in file cabinets, and money on deposit at the corner bank. For most people today, at least some of their property and communications are stored as data on a computer server and accessed via the Internet.

Collectively, a person’s digital property and electronic communications are referred to as “digital assets” and the companies that store those assets on their servers are called “custodians.” Access to digital assets is usually governed by a terms-of-service agreement rather than by property law. This creates problems when Internet users die or otherwise lose the ability to manage their own digital assets.

A fiduciary is a trusted person with the legal authority to manage another’s property, and the duty to act in that person’s best interest. The Revised Uniform Fiduciary Access to Digital Assets Act (Revised UFADAA) addresses four common types of fiduciaries:

1. Executors or administrators of deceased persons’ estates;
2. Court-appointed guardians or conservators of protected persons’ estates;
3. Agents appointed under powers of attorney; and
4. Trustees.

Revised UFADAA gives Internet users the power to plan for the management and disposition of their digital assets in a similar way as they can make plans for their tangible property. In case of conflicting instructions, the act provides a three-tiered system of priorities:

1. If the custodian provides an online tool, separate from the general terms of service, that allows the user to name another person to have access to the user’s digital assets or to direct the custodian to delete the user’s digital assets, Revised UFADAA makes the user’s online instructions legally enforceable.

2. If the custodian does not provide an online planning option, or if the user declines to use the online tool provided, the user may give legally enforceable directions for the disposition of digital assets in a will, trust, power of attorney, or other written record.

3. If the user has not provided any direction, either online or in a traditional estate plan, the terms of service for the user’s account will determine whether a fiduciary may access the user’s digital assets. If the terms of service do not address fiduciary access, the default rules of Revised UFADAA will apply.
Revised UFADAA’s default rules attempt to balance the user’s privacy interest with the fiduciary’s need for access by making a distinction between the “content of electronic communications,” the “catalogue of electronic communications,” and other types of digital assets.

The content of electronic communications includes the subject line and body of a user’s email messages, text messages, and other messages between private parties. A fiduciary may never access the content of electronic communications without the user’s consent. When necessary, a fiduciary may have a right to access a catalogue of the user’s electronic communications – essentially a list of communications showing the addresses of the sender and recipient, and the date and time the message was sent.

For example, the executor of a decedent’s estate may need to access a catalogue of the decedent’s communications in order to compile an inventory of estate assets. If the executor finds that the decedent received a monthly email message from a particular bank or credit card company, the executor can contact that company directly and request a statement of the decedent’s account.

Other types of digital assets are not communications, but intangible personal property. For example, an agent under a power of attorney who has authority to access the principal’s business files will have access under Revised UFADAA to any files stored in “the cloud” as well as those stored in file cabinets. Similarly, an executor that is distributing funds from the decedent’s bank account will also have access to the decedent’s virtual currency account (e.g. bitcoin).

Under Revised UFADAA Section 15, fiduciaries for digital assets are subject to the same fiduciary duties that normally apply to tangible assets. Thus, for example, an executor may not publish the decedent’s confidential communications or impersonate the decedent by sending email from the decedent’s account. A fiduciary’s management of digital assets may also be limited by other law. For example, a fiduciary may not copy or distribute digital files in violation of copyright law, and may not exceed the user’s authority under the account’s terms of service.

In order to gain access to digital assets, Revised UFADAA requires a fiduciary to send a request to the custodian, accompanied by a certified copy of the document granting fiduciary authority, such as a letter of appointment, court order, or certification of trust. Custodians of digital assets that receive an apparently valid request for access are immune from any liability for acts done in good faith compliance.

Revised UFADAA is an overlay statute designed to work in conjunction with a state’s existing laws on probate, guardianship, trusts, and powers of attorney. It is a vital statute for the digital age, and should be enacted by every state legislature as soon as possible.

For further information about Revised UFADAA, please contact ULC Legislative Counsel Benjamin Orzeske at 312-450-6621 or borzeske@uniformalaws.org.
AN ACT

Relating to access to digital assets.

Be It Enacted by the People of the State of Oregon:

SECTION 1. Sections 2 to 18 of this 2016 Act may be cited as the Revised Uniform Fiduciary Access to Digital Assets Act (2015).

SECTION 2. As used in sections 2 to 18 of this 2016 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 a person designated as an agent under a power of attorney in accordance with ORS 127.005 to 127.045.

(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” has the meaning given that term in ORS 125.005.

(6) “Content of an electronic communication” means information concerning the substance or meaning of the communication that:

(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 a circuit court in this state.

(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. “Digital asset” 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. 2510(12).
(13) “Electronic communication service” means a custodian that provides to a user the ability to send or receive an electronic communication.

(14) “Fiduciary” means a person that is an original, additional or successor personal representative, conservator, agent or trustee.

(15) “Information” means data, text, images, videos, sounds, codes, computer programs, software, databases and similar intelligence of any nature.

(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 the 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 or special administrator, or a person legally authorized to perform substantially the same functions.

(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. “Protected person” 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. 2510(14).

(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 person. “Trustee” 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.

SECTION 3. (1) Sections 2 to 18 of this 2016 Act apply to:

(a) A fiduciary acting under a will or power of attorney executed before, on or after the effective date of this 2016 Act;

(b) A personal representative acting for a decedent who died before, on or after the effective date of this 2016 Act;

(c) A conservatorship proceeding commenced before, on or after the effective date of this 2016 Act; and

(d) A trustee acting under a trust created before, on or after the effective date of this 2016 Act.

(2) Sections 2 to 18 of this 2016 Act apply to a custodian if the user resides in this state or resided in this state at the time of the user's death.

(3) Sections 2 to 18 of this 2016 Act do not apply to a digital asset of an employer used by an employee in the ordinary course of the employer's business.

SECTION 4. (1) 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.

(2) If a user has not used an online tool to give direction under subsection (1) of this section, 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.

(3) A user's direction under subsection (1) or (2) of this section 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. (1) Sections 2 to 18 of this 2016 Act do 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.

(2) Sections 2 to 18 of this 2016 Act do not give a fiduciary or a 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.

(3) 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 of this 2016 Act.

SECTION 6. (1) When disclosing digital assets of a user under sections 2 to 18 of this 2016 Act, the custodian may, in the custodian's sole discretion:

(a) Grant a fiduciary or designated recipient full access to the user's account;
(b) 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
(c) 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.

(2) A custodian may assess a reasonable administrative charge for the cost of disclosing digital assets under sections 2 to 18 of this 2016 Act.

(3) A custodian need not disclose under sections 2 to 18 of this 2016 Act a digital asset deleted by a user.

(4) If a user directs, or a fiduciary requests, a custodian to disclose some, but not all, of the user's digital assets under sections 2 to 18 of this 2016 Act, the custodian need not disclose the digital assets if segregation of the digital 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:

(a) A subset limited by date of the user's digital assets;
(b) All of the user's digital assets to the fiduciary or designated recipient;
(c) None of the user's digital assets; or
(d) All of the user's digital assets to the court for review in camera.

SECTION 7. If a deceased user consented to, or a court directs, disclosure of the content 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 personal 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 personal 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, user name, 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:  
   (A) The user had a specific account with the custodian, identifiable by the information specified in paragraph (a) of this subsection;  
   (B) Disclosure of the content of electronic communications of the user would not violate 18 U.S.C. 2701 et seq., 47 U.S.C. 222 or other applicable law;  
   (C) Unless the user provided direction using an online tool, the user consented to disclosure of the content of electronic communications; or  
   (D) Disclosure of the content of electronic communications of the user is reasonably necessary for administration of the estate.

SECTION 8. 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 personal 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 personal representative or a small estate affidavit or court order; and  
   (4) If requested by the custodian:  
      (a) A number, user name, 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:  
         (A) The user had a specific account with the custodian, identifiable by the information specified in paragraph (a) of this subsection; or  
         (B) Disclosure of the user’s digital assets is reasonably necessary for administration of the estate.

SECTION 9. 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, user name, 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. Unless otherwise ordered by the court, directed by the principal or provided in 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, user name, 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. 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. 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 ORS 130.860 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, user name, 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. 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 court order that gives the conservator authority over the digital assets of a protected person.

SECTION 14. (1) After an opportunity for a hearing, the court may grant a conservator access to the digital assets of a protected person.

   (2) Unless otherwise ordered by the court or directed by the user, a custodian shall disclose to the 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:

   (a) A written request for disclosure in physical or electronic form;
   (b) A certified copy of the court order that gives the conservator authority over the digital assets of the protected person; and
(c) If requested by the custodian:
(A) A number, user name, 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.
(3) 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 the account of the protected person for good cause. A request made under this subsection must be accompanied by a certified copy of the court order giving the conservator authority over the protected person's property.

SECTION 15. (1) The legal duties imposed on a fiduciary charged with managing tangible property apply to the management of digital assets, including:
(a) The duty of care;
(b) The duty of loyalty; and
(c) The duty of confidentiality.
(2) A fiduciary’s or designated recipient’s authority with respect to a digital asset of a user:
(a) Except as otherwise provided in section 4 of this 2016 Act, is subject to the applicable terms of service;
(b) Is subject to other applicable law, including copyright law;
(c) In the case of a fiduciary, is limited by the scope of the fiduciary’s duties; and
(d) May not be used to impersonate the user.
(3) 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 has a right or interest and that is not held by a custodian or subject to a terms-of-service agreement.
(4) 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 laws on unauthorized computer access.
(5) A fiduciary with authority over the tangible, personal property of a decedent, protected person, principal or settlor:
(a) Has the right to access the property and any digital asset stored in the property; and
(b) Is an authorized user for the purpose of computer fraud and unauthorized computer access laws, including this state’s laws on unauthorized computer access.
(6) 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.
(7) 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:
(a) If the user is deceased, a certified copy of the death certificate of the user;
(b) A certified copy of the letter of appointment of the personal representative, a small estate affidavit or court order, a court order, a power of attorney or a trust giving the fiduciary authority over the account; and
(c) If requested by the custodian:
(A) A number, user name, 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) of this paragraph.

SECTION 16. (1) Not later than 60 days after receipt of the information required under sections 7 to 15 of this 2016 Act, a custodian shall comply with a request 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.

(2) An order under subsection (1) of this section directing compliance must contain a finding that compliance is not in violation of 18 U.S.C. 2702.

(3) A custodian may notify the user that a request for disclosure or to terminate an account was made under sections 2 to 18 of this 2016 Act.

(4) A custodian may deny a request under sections 2 to 18 of this 2016 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.

(5) Sections 2 to 18 of this 2016 Act do not limit a custodian's ability to obtain or require a fiduciary or designated recipient requesting disclosure or termination to obtain a court order that:

(a) Specifies that an account belongs to the protected person or principal;
(b) Specifies that there is sufficient consent from the protected person or principal to support the requested disclosure; and
(c) Contains a finding required by law other than under sections 2 to 18 of this 2016 Act.

(6) A custodian and the custodian’s officers, employees and agents are immune from liability for an act or omission done in good faith in compliance with sections 2 to 18 of this 2016 Act.

SECTION 17. 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 the enacting 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

WITH PREFATORY NOTE AND COMMENTS

Copyright © 2015 By NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS

March 8, 2016
ABOUT ULC

The Uniform Law Commission (ULC), also known as National Conference of Commissioners on Uniform State Laws (NCCUSL), now in its 124th year, provides states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law.

ULC members must be lawyers, qualified to practice law. They are practicing lawyers, judges, legislators and legislative staff and law professors, who have been appointed by state governments as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands to research, draft and promote enactment of uniform state laws in areas of state law where uniformity is desirable and practical.

- ULC strengthens the federal system by providing rules and procedures that are consistent from state to state but that also reflect the diverse experience of the states.
- ULC statutes are representative of state experience, because the organization is made up of representatives from each state, appointed by state government.
- ULC keeps state law up-to-date by addressing important and timely legal issues.
- ULC’s efforts reduce the need for individuals and businesses to deal with different laws as they move and do business in different states.
- ULC’s work facilitates economic development and provides a legal platform for foreign entities to deal with U.S. citizens and businesses.
- Uniform Law Commissioners donate thousands of hours of their time and legal and drafting expertise every year as a public service, and receive no salary or compensation for their work.
- ULC’s deliberative and uniquely open drafting process draws on the expertise of commissioners, but also utilizes input from legal experts, and advisors and observers representing the views of other legal organizations or interests that will be subject to the proposed laws.
- ULC is a state-supported organization that represents true value for the states, providing services that most states could not otherwise afford or duplicate.
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (2015)

The Committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this Act consists of the following individuals:

SUZANNE BROWN WALSH, 185 Asylum St., Hartford, CT 06103-3469, Chair
TURNEY P. BERRY, 500 W. Jefferson St., Suite 2800, Louisville, KY 40202
DAVID D. BIKLEN, 799 Prospect Ave., B2, West Hartford, CT 06105
STEPHEN Y. CHOW, 125 Summer St., Boston, MA 02110-1624
VINCENT C. DELIBERATO, Legislative Reference Bureau, Main Capitol Bldg., Room 641,
Harrisburg, PA 17120-0033
MARC S. FEINSTEIN, 431 N. Phillips Ave., Suite 301, Sioux Falls, ND 57104
GENE H. HENNIG, 500 IDS Center, 80 S. 8th St., Minneapolis, MN 55402-3796
STANLEY C. KENT, 90 S. Cascade Ave., Suite 1210, Colorado Springs, CO 80903
SUSAN K. NICHOLS, 3217 Northampton St., Raleigh, NC 27609-0625
DANIEL ROBBINS, 15301 Ventura Blvd., Bldg. E, Sherman Oaks, CA 91403
LANE SHETTERLY, 189 SW Academy St., P.O. Box 105, Dallas, OR 97338
NAOMI CAHN, George Washington University School of Law, 2000 H St. NW, Washington,
DC 20052, Reporter

EX OFFICIO
HARRIET LANSING, 1 Heather Pl., St. Paul, MN 55102-3017, President
GAIL HAGERTY, South Central Judicial District, P.O. Box 1013, 514 E. Thayer Ave.,
Bismarck, ND 58502-1013, Division Chair

EXECUTIVE DIRECTOR
LIZA KARSAI, 111 N. Wabash Ave., Suite 1010, Chicago, IL 60602, Executive Director

Copies of this act may be obtained from:
NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org
# REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (2015)

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFATORY NOTE</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>SECTION 1</td>
<td>SHORT TITLE.</td>
<td>3</td>
</tr>
<tr>
<td>SECTION 2</td>
<td>DEFINITIONS.</td>
<td>3</td>
</tr>
<tr>
<td>SECTION 3</td>
<td>APPLICABILITY.</td>
<td>8</td>
</tr>
<tr>
<td>SECTION 4</td>
<td>USER DIRECTION FOR DISCLOSURE OF DIGITAL ASSETS.</td>
<td>10</td>
</tr>
<tr>
<td>SECTION 5</td>
<td>TERMS-OF-SERVICE AGREEMENT.</td>
<td>11</td>
</tr>
<tr>
<td>SECTION 6</td>
<td>PROCEDURE FOR DISCLOSING DIGITAL ASSETS</td>
<td>12</td>
</tr>
<tr>
<td>SECTION 7</td>
<td>DISCLOSURE OF CONTENT OF ELECTRONIC COMMUNICATIONS OF DECEASED USER.</td>
<td>13</td>
</tr>
<tr>
<td>SECTION 8</td>
<td>DISCLOSURE OF OTHER DIGITAL ASSETS OF DECEASED USER.</td>
<td>16</td>
</tr>
<tr>
<td>SECTION 9</td>
<td>DISCLOSURE OF CONTENT OF ELECTRONIC COMMUNICATIONS OF PRINCIPAL.</td>
<td>17</td>
</tr>
<tr>
<td>SECTION 10</td>
<td>DISCLOSURE OF OTHER DIGITAL ASSETS OF PRINCIPAL.</td>
<td>18</td>
</tr>
<tr>
<td>SECTION 11</td>
<td>DISCLOSURE OF DIGITAL ASSETS HELD IN TRUST WHEN TRUSTEE IS ORIGINAL USER.</td>
<td>19</td>
</tr>
<tr>
<td>SECTION 12</td>
<td>DISCLOSURE OF CONTENTS OF ELECTRONIC COMMUNICATIONS HELD IN TRUST WHEN TRUSTEE NOT ORIGINAL USER.</td>
<td>19</td>
</tr>
<tr>
<td>SECTION 13</td>
<td>DISCLOSURE OF OTHER DIGITAL ASSETS HELD IN TRUST WHEN TRUSTEE NOT ORIGINAL USER.</td>
<td>21</td>
</tr>
<tr>
<td>SECTION 14</td>
<td>DISCLOSURE OF DIGITAL ASSETS TO [CONSERVATOR] OF [PROTECTED PERSON].</td>
<td>22</td>
</tr>
<tr>
<td>SECTION 15</td>
<td>FIDUCIARY DUTY AND AUTHORITY.</td>
<td>23</td>
</tr>
<tr>
<td>SECTION 16</td>
<td>CUSTODIAN COMPLIANCE AND IMMUNITY.</td>
<td>28</td>
</tr>
<tr>
<td>SECTION 17</td>
<td>UNIFORMITY OF APPLICATION AND CONSTRUCTION.</td>
<td>30</td>
</tr>
<tr>
<td>SECTION 18</td>
<td>RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT.</td>
<td>30</td>
</tr>
<tr>
<td>[SECTION 19. SEVERABILITY.]</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>SECTION 20</td>
<td>REPEALS; CONFORMING AMENDMENTS.</td>
<td>31</td>
</tr>
<tr>
<td>SECTION 21</td>
<td>EFFECTIVE DATE.</td>
<td>31</td>
</tr>
</tbody>
</table>
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT (2015)

PREFATORY NOTE

The purpose of the Revised Fiduciary Access to Digital Assets Act (Revised UFADAA) is twofold. First, it gives fiduciaries the legal authority to manage digital assets and electronic communications in the same way they manage tangible assets and financial accounts, to the extent possible. Second, it gives custodians of digital assets and electronic communications legal authority to deal with the fiduciaries of their users, while respecting the user’s reasonable expectation of privacy for personal communications. The general goal of the act is to facilitate fiduciary access and custodian disclosure while respecting the privacy and intent of the user. It adheres to the traditional approach of trusts and estates law, which respects the intent of an account holder and promotes the fiduciary’s ability to administer the account holder’s property in accord with legally-binding fiduciary duties. The act removes barriers to a fiduciary’s access to electronic records and property and leaves unaffected other law, such as fiduciary, probate, trust, banking, investment securities, agency, and privacy law. Existing law prohibits any fiduciary from violating fiduciary responsibilities by divulging or publicizing any information the fiduciary obtains while carrying out his or her fiduciary duties.

Revised UFADAA addresses four different types of fiduciaries: personal representatives of decedents’ estates, conservators for protected persons, agents acting pursuant to a power of attorney, and trustees. It distinguishes the authority of fiduciaries, which exercise authority subject to this act only on behalf of the user, from any other efforts to access the digital assets. Family members or friends may seek such access, but, unless they are fiduciaries, their efforts are subject to other laws and are not covered by this act.

Digital assets are electronic records in which individuals have a right or interest. As the number of digital assets held by the average person increases, questions surrounding the disposition of these assets upon the individual’s death or incapacity are becoming more common. These assets, ranging from online gaming items to photos, to digital music, to client lists, can have real economic or sentimental value. Yet few laws exist on the rights of fiduciaries over digital assets. Holders of digital assets may not consider the fate of their online presences once they are no longer able to manage their assets, and may not expressly provide for the disposition of their digital assets or electronic communications in the event of their death or incapacity. Even when they do, their instructions may come into conflict with custodians’ terms-of-service agreements. Some Internet service providers have explicit policies on what will happen when an individual dies, while others do not, and even where these policies are included in the terms-of-service agreement, consumers may not be fully aware of the implications of these provisions in the event of death or incapacity or how courts might resolve a conflict between such policies and a will, trust instrument, or power of attorney.

The situation regarding fiduciaries’ access to digital assets is less than clear, and is subject to federal and state privacy and computer “hacking” laws as well as state probate law. A minority of states has enacted legislation on fiduciary access to digital assets, and numerous other states have considered, or are considering, legislation. Existing legislation differs with
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

With regard to the general scope of the act, the act’s coverage is inherently limited by the definition of “digital assets.” The act applies only to electronic records in which an individual has a property right or interest, which do not include the underlying asset or liability unless it is itself an electronic record.

The act is divided into 21 sections. Section 2 contains definitions of terms used throughout the act.

Section 3 governs applicability, clarifying the scope of the act and the fiduciaries who have access to digital assets under Revised UFADAA, and carves out an exception for digital assets of an employer used by an employee during the ordinary course of business.

Section 4 provides ways for users to direct the disposition or deletion of their digital assets at their death or incapacity, and establishes a priority system in case of conflicting instructions.

Section 5 establishes that the terms-of-service governing an online account apply to fiduciaries as well as to users, and clarify that a fiduciary cannot take any action that the user could not have legally taken.

Section 6 gives the custodians of digital assets a choice for disclosing those assets to fiduciaries. A custodian may, but need not, comply with a request for access by allowing the fiduciary to reset the password and access the user’s account. In many cases that will be the simplest method of compliance. However, a custodian may also comply without giving access to a user’s account by simply giving a copy of all the user’s digital assets to the fiduciary. That method may be preferred for a social media account when a fiduciary has no need for full access and control.

Sections 7-14 establish the rights of personal representatives, conservators, agents acting pursuant to a power of attorney, and trustees. Each of the fiduciaries is subject to different rules for the content of communications protected under federal privacy laws and for other types of digital assets. Generally, a fiduciary will have access to a catalogue of the user’s communications, but not the content, unless the user consented to the disclosure of the content.

Section 15 contains general provisions relating to the rights and responsibilities of the fiduciary. Section 16 addresses compliance by custodians and grants immunity for any acts taken in order to comply with a fiduciary’s request under this act. Sections 17-21 address miscellaneous topics, including retroactivity, the effective date of the act, and similar issues.
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).

**Comment**

Many of the definitions are based on those in the Uniform Probate Code: agent (UPC Section 1-201(1)), conservator (UPC Section 5-102(1)), court (UPC Section 1-201(8)), electronic (UPC Section 5B-102(3)), fiduciary (UPC Section 1-201(15)), person (UPC Section 5B-101(6)), personal representative (UPC Section 1-201(35)), power of attorney (UPC Section 5B-102(7)), principal (UPC Section 5B-102(9)), protected person (UPC Section 5-102(8)), record (UPC Section 1-201(41)), and will (UPC Section 1-201(57)). The definition of “information” is based on that in the Uniform Electronic Transactions Act, Section 2, subsection (11). Many of the other definitions are either drawn from federal law, as discussed below, or are new for this act.

The definition of “account” is broadly worded to encompass any contractual arrangement subject to a terms-of-service agreement, but limited for the purpose of this act by the requirement that the custodian carry, maintain, process, receive, or store a digital asset of the user.

The definition of “digital asset” expressly excludes underlying assets such as funds held in an online bank account. Because records may exist in both electronic and non-electronic formats, this definition clarifies the scope of the act and the limitation on the type of records to which it applies. The term includes types of electronic records currently in existence and yet to be invented. It includes any type of electronically-stored information, such as: 1) information stored on a user’s computer and other digital devices; 2) content uploaded onto websites; and 3) rights in digital property. It also includes records that are either the catalogue or the content of an electronic communication. See 18 U.S.C. Section 2702(a)(2); James D. Lamm, Christina L. Kunz, Damien A. Riehl and Peter John Rademacher, *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. Miami L. Rev. 385, 388 (2014) (available at: http://goo.gl/T9jX1d).

The term “catalogue of electronic communications” is designed to cover log-type information about an electronic communication such as the email addresses of the sender and the recipient, and the date and time the communication was sent.

The term “content of an electronic communication” is adapted from 18 U.S.C. Section 2510(8), which provides that content: “when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.” The definition is designed to cover only content subject to the coverage of Section 2702 of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. Section 2510 et seq.; it does not include content not subject to ECPA. Consequently, the “content of an electronic communication”, as used later throughout Revised UFADAA, refers only to information in the body of an electronic message that is not readily accessible to
the public; if the information were readily accessible to the public, it would not be subject to the privacy protections of federal law under ECPA. See S. Rep. No. 99-541, at 36 (1986). Example: X uses a Twitter account to send a message. If the tweet is sent only to other people who have been granted access to X’s tweets, then it meets Revised UFADAA’s definition of “content of an electronic communication.” But, if the tweet is completely public with no access restrictions, then it does not meet the act’s definition of “content of an electronic communication.” ECPA does not apply to private e-mail service providers, such as employers and educational institutions. See 18 U.S.C. Section 2702(a)(2); James D. Lamm, Christina L. Kunz, Damien A. Riehl and Peter John Rademacher, The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property, 68 U. Miami L. Rev. 385, 404 (2014) (available at: http://goo.gl/T9jX1d).

A “user” is a person that has an account with a custodian, and includes a deceased individual that entered into the agreement while alive. A fiduciary can be a user when the fiduciary opens the account.

The definition of “carries” is drawn from federal law, 47 U.S.C. Section 1001(8).

A “custodian” includes any entity that provides or stores electronic data for a user.

The fiduciary’s access to a record defined as a “digital asset” does not mean the fiduciary owns the asset or may engage in transactions with the asset. Consider, for example, a fiduciary’s legal rights with respect to funds in a bank account or securities held with a broker or other custodian, regardless of whether the bank, broker, or custodian has a brick-and-mortar presence. This act affects electronic records concerning the bank account or securities, but does not affect the authority to engage in transfers of title or other commercial transactions in the funds or securities, even though such transfers or other transactions might occur electronically. Revised UFADAA only deals with the right of the fiduciary to access all relevant electronic communications and digital assets accessible through the online account. An entity may not refuse to provide access to online records any more than the entity can refuse to provide the fiduciary with access to hard copy records.

An “electronic communication” is a particular type of digital asset subject to the privacy protections of the Electronic Communications Privacy Act. It includes email, text messages, instant messages, and any other electronic communication between private parties. The definition of “electronic communication” is that set out in 18 U.S.C. Section 2510(12): “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(C) any communication from a tracking device (as defined in section 3117 of this title);

or

(D) electronic funds transfer information stored by a financial institution in a
communications system used for the electronic storage and transfer of funds.

The definition of “electronic-communication service” is drawn from 18 U.S.C. Section 2510(15): “any service which provides to users thereof the ability to send or receive wire or electronic communications.” The definition of “remote-computing service” is adapted from 18 U.S.C. Section 2711(2): “the provision to the public of computer storage or processing services by means of an electronic communications system.” The definition refers to 18 U.S.C. Section 2510(14), which defines an electronic communications system as: “any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.”

A “fiduciary” under this act occupies a status recognized by state law, and a fiduciary’s powers under this act are subject to the relevant limits established by other state laws.

An “online tool” is a mechanism by which a user names an individual to manage the user’s digital assets after the occurrence of a future event, such as the user’s death or incapacity. The named individual is referred to as the “designated recipient” in the act to differentiate the person from a fiduciary. A designated recipient may perform many of the same tasks as a fiduciary, but is not held to the same legal standard of conduct.

The term “record” includes information available on both tangible and electronic media. Revised UFADAA applies only to electronic records.

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

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.

Comment

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

Subsection (a)(2) covers the situations in which a decedent dies intestate, so it falls
outside of subsection (a)(1), as well as the situations in which a state’s procedures for small
estates are used.

Subsection (b) states that custodians are subject to the act if the custodian’s user was a
resident of the enacting state. This includes out-of-state custodians, who must respond to
requests for access in the same way that out-of-state banks or credit card companies must
respond to requests from a fiduciary requesting access to a customer’s account.

Subsection (c) clarifies that the act does not apply to a fiduciary’s access to an
employer’s internal email system.

Example 1—Fiduciary access to an employee e-mail account. D dies, employed by
Company Y. Company Y has an internal e-mail communication system, available only to Y’s
employees, and used by them in the ordinary course of Y’s business. D’s personal
representative, R, believes that D used Company Y’s e-mail system to effectuate some financial
transactions that R cannot find through other means. R requests access from Company Y to the
e-mails.

Company Y is not a custodian subject to the act. Under Section 2(8), a custodian must
carry, maintain or store a user’s digital assets. A user, under Section 2(26) must have an
account, and an account, in turn, is defined under Section 2(1) as a contractual arrangement subject to a terms-of-service agreement. Company Y, like most employers, did not enter into a terms-of-service agreement with D, so Y is not a custodian.

Example 2—Employee of electronic-communication service provider. D dies, employed by Company Y. Company Y is an electronic-communication service provider. Company Y has an internal e-mail communication system, available only to Y’s employees and used by them in the ordinary course of Y’s business. D used the internal Company Y system. When not at work, D also used an electronic-communication service system that Company Y provides to the public. D’s personal representative, R, believes that D used Company Y’s internal e-mail system as well as Company Y’s electronic-communication system available to the public to effectuate some financial transactions. R seeks access to both communication systems.

As is true in Example 1, Company Y is not a custodian subject to the act for purposes of the internal email system. The situation is different with respect to R’s access to Company Y’s system that is available to the public. Assuming that Company Y can disclose the communications under federal law and R meets the other requirements of this act, Company Y must disclose them to R.

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.
Comment

This section addresses the relationship of online tools, other records documenting the user’s intent, and terms-of-service agreements. In some instances, there may be a conflict between the directions provided by a user in an online tool that limits access by other parties to the user’s digital assets, and the user’s estate planning or other personal documents that purport to authorize access for specified persons in identified situations. The act attempts to balance these interests by establishing a three-tier priority system for determining the user’s intent with respect to any digital asset.

Subsection (a) gives top priority to a user’s wishes as expressed using an online tool. If a custodian of digital assets allows the user to provide directions for handling those digital assets in case of the user’s death or incapacity, and the user does so, that provides the clearest possible indication of the user’s intent and is specifically limited to those particular digital assets.

If the user does not give direction using an online tool, but makes provisions in an estate plan for the disposition of digital assets, subsection (b) gives legal effect to the user’s directions. The fiduciary charged with managing the user’s digital assets must provide a copy of the relevant document to the custodian when requesting access. See Sections 7 through 14.

If the user provides no other direction, the terms-of-service governing the account will apply. If the terms-of-service do not address fiduciary access to digital assets, the default rules provided in this act will apply.

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.

Comment

This section clarifies that, to the extent that a custodian gives a fiduciary access to an account pursuant to Section 6, the account’s terms-of-service agreement applies equally to the
original user and to a fiduciary acting for the original user. A fiduciary is subject to the same terms and conditions of the user’s agreement with the custodian. This section does not require a custodian to permit a fiduciary to assume a user’s terms-of-service agreement if the custodian can otherwise comply with Section 6.

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
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

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

Comment

This section governs a custodian’s response to a request for disclosure of a user’s digital assets.

Subsection (a) gives the custodian of digital assets a choice of methods for disclosing digital assets to an authorized fiduciary. Each custodian has a different business model and may prefer one method over another.

Subsection (b) allows a custodian to assess a reasonable administrative charge for the cost of disclosure. This is intended to be analogous to the charge any business may assess for administrative tasks outside the ordinary course of its business to comply with a court order.

Subsection (c) states that any digital asset deleted by the user need not be disclosed, even if recoverable by the custodian. Deletion is assumed to be a good indication that the user did not intend for a fiduciary to have access.

Subsection (d) addresses requests that are unduly burdensome because they require segregation of digital assets. For example, a fiduciary’s request for disclosure of “any email pertaining to financial matters” would require a custodian to sort through the full list of emails and cull any irrelevant messages before disclosure. If a custodian receives an unduly burdensome request of this sort, it may decline to disclose the digital assets, and either the fiduciary or custodian may seek guidance from a court.

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).

Comment

The Electronic Communications Privacy Act (ECPA) distinguishes between the permissible disclosure of the “content” of an electronic communication, covered in 18 U.S.C. Section 2702(b), and of “a record or other information pertaining to a” subscriber or customer, covered in 18 U.S.C. Section 2702(c); see Matthew J. Tokson, The Content/Envelope Distinction in Internet Law, 50 Wm. & Mary L. Rev. 2105 (2009). Section 7 concerns disclosure of content;
Section 8 covers disclosure of non-content and other digital assets of the user.

Content-based material can, in turn, be divided into two types of communications: those received by the user and those sent. Federal law, 18 U.S.C. Section 2702(b) permits a custodian to 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” or “(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.”

Consequently, when the user is the “addressee or intended recipient,” material can be disclosed either to that individual or to an agent for that person, 18 U.S.C. Section 2702(b)(1), and it can also be disclosed to third parties with the “lawful consent” of the addressee or intended recipient. 18 U.S.C. Section 2702(b)(3). Material for which the user is the “originator” (or the “subscriber” to a remote computing service) can be disclosed to third parties only with the user’s “lawful consent.” 18 U.S.C. Section 2702(b)(3). (Note that, when the user is the addressee or intended recipient, material can be disclosed under either (b)(1) or (b)(3), but that when the user is the originator, lawful consent is required under (b)(3).) See the Comments concerning the definition of “content” after Section 2. By contrast to content-based material, non-content material can be disclosed either with the lawful consent of the user or to any person (other than a governmental entity) even without lawful consent. This information includes material about any communication sent, such as the addressee, sender, date/time, and other subscriber data, which this act defines as the “catalogue of electronic communications.” (Further discussion of this issue and examples are set out in the Comments to Section 15, infra.)

Therefore, Section 7 gives the personal representative access to digital assets if the user consented to disclosure or if a court orders disclosure. To obtain access, the personal representative must provide the documentation specified by Section 7. First, the personal representative must give the custodian a written request for disclosure, a copy of the death certificate, a document establishing the authority of the personal representative, and, in the absence of an online tool, a record evidencing the user’s consent to disclosure. When requesting disclosure, the fiduciary must write or email the custodian. The form of the request is limited, and does not, for example, include video, Tweet, instant message or other forms of communication.

Second, if the custodian requests, then the personal representative can be required to establish that the requested information is necessary for estate administration and the account is attributable to the decedent. Different custodians may have different procedures. Thus a custodian may request that the personal representative obtain a court order, and such an order must include findings that: 1) the user had a specific account with the custodian, 2) that disclosure of the content of electronic communications of the user would not violate the SCA or other law, 3) unless the user provided direction using an online tool, that the user consented to disclosure of the content of electronic communications, or 4) that disclosure of the content of electronic communications of a user is reasonably necessary for administration of the estate.
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.
Comment

As in Section 7, when requesting disclosure of non-content, the fiduciary must write or email the custodian.

Section 8 requires disclosure of all other digital assets, unless prohibited by the decedent or directed by the court, once the personal representative provides a written request, a death certificate and a certified copy of the letter of appointment. In addition, the custodian may request a court order, and such an order must include findings that the decedent had a specific account with the custodian and that disclosure of the decedent’s digital assets is reasonably necessary for administration of the estate. Thus, Section 8 was intended to give personal representatives default access to the “catalogue” of electronic communications and other digital assets not protected by federal privacy law.

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.

Comment

An agent has access to the content of electronic communications only when the power of attorney explicitly grants access. Section 10 concerns disclosure of other digital assets of the principal.
When a power of attorney contains the consent of the principal, ECPA does not prevent the agent from exercising authority over the content of an electronic communication. See the Comments to Section 7. There should be no question that an explicit delegation of authority in a power of attorney constitutes authorization from the user to access digital assets and provides “lawful consent” to allow disclosure of the content of an electronic communication from an electronic-communication service or a remote-computing service pursuant to applicable law. Both authorization and lawful consent are important because 18 U.S.C. Section 2701 deals with intentional access without authorization and 18 U.S.C. Section 2702 allows a service provider to disclose with lawful consent. Federal courts have not yet interpreted how ECPA affects a fiduciary’s efforts to access the content of an electronic communication. E.g., In re Facebook, Inc., 923 F. Supp. 2d 1204 (N.D. Cal. 2012).

When requesting access, the agent must write or email the custodian (see the comments in Section 7). The agent must also give the custodian an original or copy of the power of attorney expressly granting the agent authority over the contents of electronic communications of the principal to the agent and a certification by the agent, under penalty of perjury, that the power of attorney is in effect. In addition, if requested by the custodian, the agent must provide a unique subscriber or account identifier assigned by the custodian to identify the principal’s account or other 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.

Comment

This section establishes that the agent has default authority over all of the principal’s digital assets, other than the content of the principal’s electronic communications. When requesting access, the agent must write or email the custodian (see the comments in Section 7).

The agent must also give the custodian an original or copy of the power of attorney and a certification by the agent, under penalty of perjury, that the power of attorney is in effect. Also, if requested by the custodian, the agent must provide a unique subscriber or account identifier assigned by the custodian to identify the principal’s account, or some 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.

Comment

Section 11 provides that trustees who are original users can access all digital assets held in the trust. There should be no question that a trustee who is the original user will have full access to all digital assets. This includes the content of electronic communications, as access to content is presumed with respect to assets for which the trustee is the initial user. A trustee may have title to digital assets when the trustee opens an account as trustee; under those circumstances, the trustee can access the content of each digital asset that is in an account for which the trustee is the original user, not necessarily each digital asset held in the trust.

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,
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

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.

Comment

For accounts that are transferred into a trust by the settlor or in another manner, a trustee is not the original user of the account, and the trustee’s authority is qualified. Thus, Section 12, governing disclosure of content of electronic communications from those accounts, requires consent.

Section 12 addresses situations involving an inter vivos transfer of a digital asset into a trust, a transfer into a testamentary trust, or a transfer via a pourover will or other governing instrument of a digital asset into a trust. In those situations, a trustee becomes a successor user when the settlor transfers a digital asset into the trust. There should be no question that the trustee with legal title to the digital asset was authorized by the settlor to access the digital assets so transferred, including both the catalogue and content of an electronic communication, and this provides “lawful consent” to allow disclosure of the content of an electronic communication from an electronic-communication service or a remote-computing service pursuant to applicable law. See the Comments concerning the definitions of the “content of an electronic communication” after Section 2. Nonetheless, Sections 12 and 13 distinguish between the catalogue and content of an electronic communication in case there are any questions about whether the form in which property transferred into a trust is held constitutes lawful consent. Both authorization and lawful consent are important because 18 U.S.C. Section 2701 deals with intentional access without authorization and because 18 U.S.C. Section 2702 allows a service provider to disclose with lawful consent.
The underlying trust documents and default trust law will supply the allocation of responsibilities between and among trustees. When requesting access, the trustee must write or email the custodian (see comments to Section 7). The trustee must also give the custodian an original or copy of the trust that includes consent to disclosure of the content of electronic communications to the trustee and a certification by the trustee, under penalty of perjury, that the trust exists and that the trustee is a currently acting trustee of the trust. Also, if requested by the custodian, the trustee must provide a unique subscriber or account identifier assigned by the custodian to identify the trust’s account, or some 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]]; and

(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.

Comment

Section 13 governs digital assets other than the contents of electronic communications, so it does not require the settlor’s consent.
When requesting access, the trustee must write or email the custodian (see Comments to Section 7).

The trustee must also give the custodian an original or copy of the trust, and a certification by the trustee, under penalty of perjury, that the trust exists and that the trustee is a currently acting trustee of the trust. Also, if requested by the custodian, the trustee must provide a unique subscriber or account identifier assigned by the custodian to identify the trust’s account, or some 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.

**Comment**

When a conservator is appointed to represent a protected person’s interests, the protected person may still retain some right to privacy in their personal communications. Therefore, Section 14 does not permit conservators to request disclosure of a protected person’s electronic communications on the basis of the conservatorship order alone. To access a protected person’s digital assets and a catalogue of electronic communications, a conservator must be specifically authorized by the court to do so. This requirement for express judicial authority over digital assets does not limit the fiduciary’s authority over the underlying assets, such as funds held in a bank account. The meaning of the term “hearing” will vary from state to state according to state law and procedures.

State law will establish the criteria for when a court will grant power to the conservator. For example, UPC Section 5-411(c) requires the court to consider the decision the protected person would have made as well as a list of other factors. Existing state law may also set out the requisite standards for a conservator’s actions. The conservator must exercise authority in the interests of the protected person. When requesting access to digital assets in which the protected person has a right or interest, the conservator must write or email the custodian (see comments to Section 7).

The conservator must also give the custodian a certified copy of the court order that gives the conservator authority over the protected person’s digital assets. Also, if requested by the custodian, the conservator must provide a unique subscriber or account identifier assigned by the custodian to identify the protected person’s account, or some evidence linking the account to the protected person. The custodian is required to disclose the digital assets so requested.

Under subsection (c), a conservator with general authority to manage the assets of the protected person may request suspension or termination of the protected person’s account, for good cause.

**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].
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 “protected person” with the local term for a person subject to a conservatorship, if different.

**Comment**

The original version of UFADAA incorporated fiduciary duties by reference to “other law.” This proved to be confusing and led to enactment difficulty. Section 15 specifies the nature, extent and limitation of the fiduciary’s authority over digital assets. Subsection (a) expressly imposes all fiduciary duties to the management of digital assets, including the duties of care, loyalty and confidentiality. Subsection (b) specifies that a fiduciary’s authority over digital
assets is subject to the terms-of-service agreement, except to the extent the terms-of-service agreement provision is overridden by an action taken pursuant to Section 4, and it reinforces the applicability of copyright and fiduciary duties. Finally, subsection 15(b) prohibits a fiduciary’s authority being used to impersonate a user. Subsection 15(c) permits the fiduciary to access all digital assets not in an account or subject to a terms-of-service agreement. Subsection 15(d) further specifies that the fiduciary is an authorized user under any applicable law on unauthorized computer access.

Subsection 15(g) gives the fiduciary the option of requesting that an account be terminated, if termination would not violate a fiduciary duty.

This issue concerning the parameters of the fiduciary’s authority potentially arises in two situations: 1) the fiduciary obtains access to a password or the like directly from the user, as would be true in various circumstances such as for the trustee of an inter vivos trust or someone who has stored passwords in a written or electronic list and those passwords are then transmitted to the fiduciary; and 2) the fiduciary obtains access pursuant to this act.

This section clarifies that the fiduciary has the same authority as the user if the user were the one exercising the authority (note that, where the user has died, this means that the fiduciary has the same access as the user had immediately before death). This means that the fiduciary’s authority to access the digital asset is the same as the user except where, pursuant to Section 4, the user has explicitly opted out of fiduciary access. In exercising its responsibilities, the fiduciary is subject to the duties and obligations established pursuant to state fiduciary law, and is liable for breach of those duties. Note that even if the digital asset were illegally obtained by the user, the fiduciary would still need access in order to handle that asset appropriately. There may, for example, be tax consequences that the fiduciary would be obligated to report.

However, this section does not require a custodian to permit a fiduciary to assume a user’s terms-of-service agreement if the custodian can otherwise comply with Section 6.

In exercising its responsibilities, the fiduciary is subject to the same limitations as the user more generally. For example, a fiduciary cannot delete an account if this would be fraudulent. Similarly, if the user could challenge provisions in a terms-of-service agreement, then the fiduciary is also able to do so. See Ajemian v. Yahoo!, Inc., 987 N.E.2d 604 (Mass. 2013).

Subsection (b) is designed to establish that the fiduciary is authorized to obtain or access digital assets in accordance with other applicable laws. The language mirrors that used in Title II of the Electronic Communications Privacy Act of 1986 (ECPA), also known as the Stored Communications Act, 18 U.S.C. Section 2701 et seq. (2006); see, e.g., Orin S. Kerr, A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It, 72 Geo. Wash. L. Rev. 1208 (2004). The subsection clarifies that state law treats the fiduciary as “authorized” under state laws criminalizing unauthorized access.

State laws vary in their coverage but typically prohibit unauthorized computer access. By
defining the fiduciary as an authorized user in subsection (d), the fiduciary has authorization under applicable law to access the digital assets under state computer trespass laws.

Federal courts may look to these provisions to guide their interpretations of ECPA and the federal Computer Fraud and Abuse Act, but fiduciaries should understand that federal courts may not view such provisions as dispositive in determining whether access to a user’s account violated federal criminal law.

Subsection (e) clarifies that the fiduciary is authorized to access digital assets stored on tangible personal property of the decedent, protected person, principal, or settlor, such as laptops, computers, smartphones or storage media, exempting fiduciaries from application for purposes of state or federal laws on unauthorized computer access. For criminal law purposes, this clarifies that the fiduciary is authorized to access all of the user’s digital assets, whether held locally or remotely.

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

The personal representative of D’s estate has the authority to access D’s electronic banking statements and D’s photo account, which both fall under the act’s definition of a “digital asset.” This means that, if these accounts are password-protected or otherwise unavailable to the personal representative, then the bank and the photo account service must give access to the personal representative when the request is made in accordance with Section 8. If the terms-of-service agreement permits D to transfer the accounts electronically, then the personal representative of D’s estate can use that procedure for transfer as well.

The personal representative of D’s estate is also able to request that the e-mail account service provider grant access to e-mails sent or received by D; ECPA permits the service provider to release the catalogue to the personal representative. The service provider also must provide the personal representative access to the content of an electronic communication sent or received by D if the user has consented and the fiduciary submitted the information required under Section 7. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

**Example 2—Access to digital assets by agent.** X creates a power of attorney designating A as X’s agent. The power of attorney expressly grants A authority over X’s digital assets, including the content of an electronic communication. X has a bank account for which X receives only electronic statements, X has stored photos in a cloud-based Internet account, and X has a game character and in-game property associated with an online game. X also has an e-mail account with a company that provides electronic-communication services to the public.
A has the authority to access X’s electronic bank statements, the photo account, the game character and in-game property associated with the online game, all of which fall under the act’s definition of a “digital asset.” This means that, if these accounts are password-protected or otherwise unavailable to A as X’s agent, then the bank, the photo account service provider, and the online game service provider must give access to A when the request is made in accordance with Section 10. If the terms-of-service agreement permits X to transfer the accounts electronically, then A as X’s agent can use that procedure for transfer as well.

As X’s agent, A is also able to request that the e-mail account service provider grant access to e-mails sent or received by X; ECPA permits the service provider to release the catalogue. The service provider also must provide A access to the content of an electronic communication sent or received by X if the fiduciary provides the information required under Section 9. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 3—Access to digital assets by trustee. T is the trustee of a trust established by S. As trustee of the trust, T opens a bank account for which T receives only electronic statements. S transfers into the trust to T as trustee (in compliance with a terms-of-service agreement) a game character and in-game property associated with an online game and a cloud-based Internet account in which S has stored photos. S also transfers to T as trustee (in compliance with the terms-of-service agreement) an e-mail account with a company that provides electronic-communication services to the public.

T is an original user with respect to the bank account that T opened, and T has the ability to access the electronic banking statements under Section 11. T, as successor user to S, may under Section 13 access the game character and in-game property associated with the online game and the photo account, which both fall under the act’s definition of a “digital asset.” This means that, if these accounts are password-protected or otherwise unavailable to T as trustee, then the bank, the photo account service provider, and the online game service provider must give access to T when the request is made in accordance with the act. If the terms-of-service agreement permits the user to transfer the accounts electronically, then T as trustee can use that procedure for transfer as well.

T as successor user of the e-mail account for which S was previously the user is also able to request that the e-mail account service provider grant access to e-mails sent or received by S; and ECPA permits the service provider to release the catalogue. The service provider also must provide T access to the content of an electronic communication sent or received by S if the fiduciary provides the information required under Section 12. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

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.

**Comment**

This section establishes that custodians are protected from liability when they act in accordance with the procedures of this act and in good faith. The types of actions covered include disclosure as well as transfer of copies. The critical issue in conferring immunity is the source of the liability. Direct liability is not subject to immunity; indirect liability is subject to immunity.

Direct liability could only arise from noncompliance with a judicial order issued under sections 7 to 15. Upon determination of a right of access under those sections, a court may issue an order to grant access under section 16. Section 16(b) requires that an order directing compliance contain a finding that compliance is not in violation of 18 U.S.C. Section 2702. Noncompliance with that order would give rise to liability for contempt. There is no immunity from this liability.

Indirect liability could arise from granting a right of access under this act. Access to a digital asset might invade the privacy or the harm the reputation of the decedent, protected person, principal, or settlor, it might harm the family or business of the decedent, protected person, principal, or settlor, and it might harm other persons. The grantor of access to the digital asset is immune from liability arising out of any of these circumstances if the grantor acted in good faith to comply with this act. If there is a judicial order under section 16, compliance with the order establishes good faith. Absent a judicial order under section 16, good faith must be established by the grantor’s assessment of the requirements of this act. Further, Section 16(e) allows the custodian to verify that the account belongs to the person represented by the fiduciary.

**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 ....
October 13, 2015

Ben Orzeske
Chief Counsel
Uniform Law Commission
111 N. Wabash Ave.
Suite 1010
Chicago, IL 60602

Dear Mr. Orzeske:

I am writing to express Google’s support for the Revised Uniform Fiduciary Access to Digital Assets Act. We are pleased to have found common accord with the Uniform Law Commission in both of our efforts to address access issues to digital information of decedents and others.

The revised Uniform Act accommodates the needs of settling and administering estates, providing full or limited access to information for guardians, holders of powers of attorney and others assisting people who may be incapacitated, while respecting the account holder’s rights to privacy. In addition to commitments made to users, custodians’ obligations under the federal Electronic Communications Privacy Act prohibit disclosures of content or account information except under specific circumstances. The Uniform Act appropriately recognizes these limitations and provides a consistent framework for anyone petitioning for information related to the contents of another’s account.

Support for this legislation extends only as far as bills based on the Uniform Act remain consistent with it and we reserve the right to support or oppose individual bills based on the Uniform Act after their review.

Sincerely,

Ron Barnes
Head of State Legislative Affairs
October 12, 2015

Uniform Law Commission
111 N. Wabash Avenue
Suite 1010
Chicago, Illinois 60602

Dear Uniform Law Commission:

Facebook appreciates the work of the ULC commissioners and staff in crafting a uniform act – the Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA") – which we believe creates a reasonable compromise regarding disposition of digital accounts upon death or incapacitation. We support the enactment of RUFADAA by state legislatures.

Recognizing that this is a sensitive issue involving an extremely complicated legal landscape and each state must conform RUFADAA to its own statutes, we will need to review proposed bills individually before determining our position. Uniformity in state law on this issue is important to Facebook and we are unlikely to support language that materially differs from RUFADAA.

Again, we appreciate the hard work of the ULC on this issue.

Sincerely,

Dan Sachs
Manager, State Policy
Facebook, Inc.
## Comparison of the Uniform Fiduciary Access to Digital Assets Act (Original UFADAA), The Privacy Expectations Afterlife and Choices Act (PEAC Act), and the Revised Uniform Fiduciary Access to Digital Assets Act (Revised UFADAA)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Original UFADAA</th>
<th>PEAC Act</th>
<th>Revised UFADAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estate representative’s access to the content of a decedent’s electronic communications.</td>
<td>Permitted unless the decedent opted out while alive.</td>
<td>Not permitted unless a court finds that the decedent consented to disclosure and the estate indemnifies the custodian. The request must specifically identify the account.</td>
<td>Not permitted unless the decedent consented to disclosure. Custodian may request a court order specifically identifying the account and finding consent. Indemnification not required.</td>
</tr>
<tr>
<td>Estate representative’s access to other digital assets of a decedent.</td>
<td>Permitted unless the decedent opted out while alive.</td>
<td>Unless the decedent opted out, access to one year’s worth of records permitted with a court order only if relevant to resolve fiscal assets of the estate.</td>
<td>Permitted unless the decedent opted out or the court directs otherwise. Custodian may request a court order specifically identifying the account and finding that access is reasonably necessary for estate administration.</td>
</tr>
<tr>
<td>Conservator’s access to the content of a protected person’s electronic communications.</td>
<td>Permitted if access ordered by the court.</td>
<td>Not addressed.</td>
<td>Custodian need not disclose contents without the express consent of the protected person, but may suspend or terminate an account for good cause if requested by the conservator.</td>
</tr>
<tr>
<td>Conservator’s access to other digital assets of a protected person.</td>
<td>Permitted if access ordered by the court.</td>
<td>Not addressed.</td>
<td>Permitted if authorized by the conservatorship order. Custodian may require specific identification of the account and evidence linking the account to the protected person.</td>
</tr>
<tr>
<td>Agent’s access to the content of a principal’s electronic communications.</td>
<td>Permitted if expressly authorized by the principal.</td>
<td>Not addressed.</td>
<td>Permitted if expressly authorized by the principal. Custodian may require specific identification of the account and evidence linking the account to the principal.</td>
</tr>
<tr>
<td>Issue</td>
<td>Original UFADAA</td>
<td>PEAC Act</td>
<td>Revised UFADAA</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent’s access to other digital assets.</td>
<td>Permitted under a grant of general or specific authority.</td>
<td>Not addressed.</td>
<td>Permitted under a grant of general or specific authority. Custodian may require specific identification of the account and evidence linking the account to the principal.</td>
</tr>
<tr>
<td>Trustee’s access to the contents of electronic communications of a trust account.</td>
<td>Permitted unless prohibited by the user, trust, or court.</td>
<td>Not addressed.</td>
<td>Permitted when trustee is the original user. Also permitted when the trustee is not the original user if authorized by the trust. Custodian may require specific identification of the account and evidence linking the account to the trust.</td>
</tr>
<tr>
<td>Trustee’s access to other digital assets of the trust.</td>
<td>Permitted unless prohibited by the user, trust, or court.</td>
<td>Not addressed.</td>
<td>Permitted unless prohibited by the user, trust, or court. Custodian may require specific identification of the account and evidence linking the account to the trust.</td>
</tr>
</tbody>
</table>
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

Uniform Fiduciary Access to Digital Assets Act: What UFADAA Know

Probate & Property Magazine: Volume 29 No. 04 (Reprinted with permission of author)

Victoria Blachly

Victoria Blachly is a partner at Samuels Yoelin Kantor LLP in Portland, Oregon. She is the chair of the Oregon State Bar Digital Assets Work Group and a member of the Enactment Team for the Uniform Law Commission UFADAA Group.

In the midst of the chaos created by fiduciaries being barred from performing their required duties, the Uniform Law Commission launched a more than two-year process resulting in the Uniform Fiduciary Access to Digital Assets Act (UFADAA). UFADAA does not create new law insomuch as it mends a large gap that prohibits fiduciaries from doing their legally mandated job.

Do you have bank or investment account statements delivered to you on-line because businesses are encouraging or even pressuring customers to go paperless? Do you have hundreds if not thousands of photographs of your charming family or adorable pets stored on-line? Do you post to any on-line social media accounts that tell part of the story of your personal or professional life? What happens to those accounts or assets when you die or become incapacitated? Does your personal representative have the authority or ability to access those accounts and try to put the pieces of a financial picture back together? Can those photographs be copied and delivered to the grieving family left behind? Should certain accounts or information be deleted, particularly if a protected person is being targeted on-line or identity theft is an issue? Even if an authorized user has the password to access an on-line account, is that a fraudulent cybercrime by misrepresenting to the end user who you are? All of these questions lead to one inescapable issue: the Internet is outrunning the law.

A personal representative to an estate, a conservator for a protected person, and a trustee for a trust have a legal duty to marshal and protect assets of the decedent or protected person; however, they face significant roadblocks when dealing with on-line providers that have widely varying terms-of-service agreements or policies regarding when or if they will provide access to on-line accounts and information to duly appointed fiduciaries. Unif. Trust Code § 801 (for example, “Upon acceptance of a trusteeship, the trustee shall administer the trust in good faith, in accordance with its terms and purposes and the interests of the beneficiaries, and in accordance with [the Uniform Trust Code]”); Robert E. Calem, What Happens to Your On-line Accounts When You Die?, Techlicious (June 29, 2010), http://tinyurl.com/38vqhtx. For example, Yahoo’s terms-of-service agreement purports to provide the company with full and sole authority to delete an account on the death of the account holder—regardless of the effect that may have on the estate.

In the midst of the chaos created by barring fiduciaries from performing their required duties, the Uniform Law Commission launched a more-than-two-year process resulting in the Uniform

UFADAA is an overlay statute designed to work in conjunction with a state’s existing laws on probate, guardianship, trusts, and powers of attorney. Enacting UFADAA will simply extend a fiduciary’s existing authority over a person’s traditional assets to include the person’s digital assets, with the same fiduciary duties to act for the benefit of the represented person or estate. It is a vital statute for the digital age and should be enacted by every state legislature as soon as possible. Indeed, most states are actively pursuing the legislation in 2015.

The Uniform Law Commission Tackles “The Digital Divide”

For 124 years the Uniform Law Commission (ULC) has been providing states with “non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law.” UFADAA (2014), available at http://tinyurl.com/p7oshxl; Suzanne Brown Walsh, The Uniform Fiduciary Access to Digital Assets Act (“UFADAA”) (2014), available at http://tinyurl.com/m4xkath (credit to Walsh for coining “The Digital Divide”). The ULC is a nonprofit, unincorporated association that seeks to provide states with nonpartisan proposed legislation regarding state laws. The ULC consists of more than 300 practicing lawyers, governmental lawyers, law professors, and lawyer-legislators from the 50 states, Washington, D.C., Puerto Rico, and the U.S. Virgin Islands. It is a well-respected organization that has been highly successful in proposing uniform laws that support certainty for businesses and individuals, including the Uniform Commercial Code and the Uniform Trust Code.

In 2012 the Uniform Law Commission created a drafting committee to consider a uniform act to vest fiduciaries with the authority to manage and distribute digital assets, copy or delete digital assets, and access digital assets. The drafting committee completed its work last year, and UFADAA was approved by the ULC on July 16, 2014.

What Are Digital Assets?

In the Internet age, the nature of property and our methods of communication have changed dramatically. A generation ago, a human being delivered our mail, and we kept photos in albums, documents in file cabinets, and money on deposit at the corner bank. For most people today, at least some of their property and communications are stored as data on a computer server and accessed via the Internet. One’s digital assets are the electronic information stored on a computer or through computer-related technology. These could include digital images from photographs, electronic investment account statements, e-mails, social media accounts, bank account statements, and so on. For many, our primary means of communication is e-mail, often through multiple e-mail accounts. We tweet about the latest happenings through our on-line accounts. We keep in touch with friends and colleagues through social networking sites. We store important information and family photos on a growing array of on-line sites. We access our financial assets, such as bank accounts and brokerage accounts, over the Internet. We pay our
bills electronically. We own Internet domain names. In the aggregate, these digital assets have tremendous financial, emotional, and aesthetic value.

Nearly every individual has some type of on-line account. These accounts are used to communicate, pay bills, conduct business, create on-line personalities, and even date. Because many individuals protect such accounts by limiting access to themselves only, accounts with protected passwords can create problems when the account holder dies because no one has access to the passwords. As a result, digital assets, including on-line accounts and information, documents, or media stored on one’s computer, are often left untouched. These include photos, videos, music, medical records, legal or financial documents, web sites, blogs, social media accounts, banking information, business accounts, and any other material or data owned by an individual. Lev Grossman, The Beast with a Billion Eyes, Time, Jan. 30, 2012, http://tinyurl.com/lxp2vup (“For every minute that passes in real time, 60 hours of video are uploaded to YouTube.”). Often, these assets have economic value and should be included in the estate for tax purposes.

Digital assets can be software (Word, Excel, Turbo Tax, Quicken); stored information on a hard drive, backup drive, CD, DVD, or thumb drive; on-line presences such as web sites, blogs, and social media accounts; on-line e-mail, bank, brokerage, financial, shopping, and travel accounts; and on-line gaming pieces, photos, digital music, client lists, bitcoins, and even digital art. See Roundup: Where to Spend Your BitCoins, Time, Dec. 9, 2013, at 9 (bitcoins are being accepted more often at places like Subway shops, for airline travel on CheapAir.com, on Baidu, China’s most popular web site, and for tuition at the University of Nicosia in Cyprus); Alexandra Sifferlin, Digital Art Clicks on the Auction Block, Time, Oct. 21, 2013. Rafael Rozendaal, the “on-line king of digital art,” builds interactive web sites that draw as many as 40 million views a year. Thirty million Facebook accounts belong to dead people. The average individual has 25 passwords. Some service providers have explicit policies on what will happen when an individual dies, but most do not; even when these policies are included in the terms of service, most consumers click-through these agreements.

Collectively, a person’s digital property and electronic communications are referred to as digital assets, and the companies that store those assets on their servers are called “custodians.” Access to digital assets is usually governed by a restrictive terms-of-service agreement provided by the custodian. This creates problems when account holders die or otherwise lose the ability to manage their own digital assets. Although there is no universally accepted definition of digital assets, UFADAA defines them as electronic records, not including an underlying asset or liability unless the asset or liability is itself a record that is electronic. All digital assets, however defined, are accessed by a tangible device, such as a computer, smartphone, tablet, or a server. Jamie P. Hopkins, Afterlife in the Cloud: Managing a Digital Estate, 5 Hastings Sci. & Tech. L.J. 210, 212 (2013).

**Fiduciaries Must Have Access to Digital Accounts**

A fiduciary is a person with the legal authority to manage another’s property and the duty to act in that person’s best interests. UFADAA concerns four common types of fiduciaries:
1. executors or administrators of deceased persons’ estates,
2. court-appointed guardians or conservators of protected persons’ estates,
3. agents appointed under powers of attorney, and
4. trustees.

UFADAA gives people the power to plan for the management and disposition of their digital assets in the same way they can make plans for their tangible property: by providing instructions in a will, trust, or power of attorney. If a person fails to plan, the same court-appointed fiduciary that manages the person’s tangible assets can manage the person’s digital assets, distributing those assets to heirs or disposing of them as appropriate.

Some custodians of digital assets provide an on-line planning option by which account holders can choose to delete or preserve their digital assets after some period of inactivity. UFADAA defers to the account holder’s choice in such circumstances but overrides any provision in a click-through terms-of-service agreement that conflicts with the account holder’s express instructions.

Under UFADAA, fiduciaries who manage an account holder’s digital assets have the same right to access those assets as the account holder, but only for the limited purpose of carrying out their fiduciary duties. Thus, an executor may access a decedent’s e-mail account to make an inventory of estate assets and ultimately to close the account in an orderly manner, but may not publish the decedent’s confidential communications or impersonate the decedent by sending e-mail from the account. Moreover, a fiduciary’s management of digital assets may be limited by other law. For example, a fiduciary may not copy or distribute digital files in violation of copyright law and may not access the contents of communications protected by federal privacy laws.

To gain access to digital assets, a fiduciary must, under UFADAA, send a request to the custodian, accompanied by a certified copy of the document granting fiduciary authority, such as letters testamentary, a court order, or a certification of trust. Custodians of digital assets that receive an apparently valid request for access are immune from any liability for good faith compliance.

The reasons a duly-authorized fiduciary may need access to on-line accounts and information are varied.

**To Prevent Identity Theft**

for criminals to hack these accounts, open new credit cards, apply for jobs, and even obtain state identification cards. Thus, a fiduciary may have to monitor and protect—perhaps simply by terminating—a decedent’s on-line accounts. See Gerry W. Beyer & Naomi R. Cahn, When You Pass on, Don’t Leave the Passwords Behind: Planning for Digital Assets, Prob. & Prop., Jan./Feb. 2012, at 40. The issue of deleting on-line information has garnered international attention with the Mario Costja Gonzalez case in Spain in which the Court of Justice concluded “that a person should be able to demand that a search engine remove links ‘on the ground that that information may be prejudicial to him or that he wishes it to be ‘forgotten’ after a certain time.’” Lev Grossman, You Have the Right to Be Forgotten: A European Court Has Upheld an Increasingly Precious Principle, Time, May 15, 2014, http://tinyurl.com/ntljps.

**To Marshal and Collect Assets**

It is now virtually impossible to collect mementos, contact friends and family, or sort through financial records without access to e-mail accounts. Most creditors and banks strongly encourage customers to “go green” and receive bills and statements electronically. Frequent flyer miles and other loyalty programs accumulate through on-line systems. There are young people who conduct all of their business and, in effect, earn their livings on-line, as bloggers, authors, or entrepreneurs. Some banks and financial institutions exist solely on-line, with no brick-and-mortar branches. Both digital and nondigital accounts may be subject to Internet-based service agreements. Although the assets themselves can be available to the executor or agent, their management and transfer may require compliance with those agreements. Digital assets themselves can have significant monetary value. The most obvious example is Bitcoin, a digital currency. See Bitcoin Home Page, https://bitcoin.org/en/ (last visited Nov. 25, 2014). The domain name “Insure.com” sold for $16 million in 2009, “sex.com” sold for $14 million in 2006, and “Fund.com” sold for £9.99 million in 2008, to name just a few. Chris Irvine, Top 10 Most Expensive Domain Names, The Telegraph, Mar. 10, 2010, http://tinyurl.com/yg4y337.

Yahoo Mail considers an account to be private property and will not hand over account information to the decedent’s family members without legal action. Peggy Hoyt & Sarah Aumiller, Estate Planning for Your On-line Identity, Estate and Business Planning Blog (June 9, 2010), http://tinyurl.com/oxzhutg. In addition, Yahoo Mail will permanently delete all accounts and their contents, preventing access to anyone, on receipt of a copy of a death certificate. Calem, What Happens to Your On-line Accounts When You Die?, supra. In fact, Yahoo’s terms of service include a “no right of survivorship and non-transferability clause.” The clause states: “You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.” Id. Such unilateral control may be directly contrary to the decedent’s intent.

With billions of dollars in unclaimed bank accounts (and other assets) finding their way to state treasurers every year, a lack of information through digital accounts will only increase this amount. Saabira Chaudhuri, The 25 Documents You Need Before You Die, Wall St. J., July 2, 2011 (“According to the National Association of Unclaimed Property Administrators, state treasurers currently hold $32.9 billion in unclaimed bank accounts and other assets.”).
To Console Grieving Loved Ones

Stories abound of grieving family members and friends searching for answers, comfort, and support in the social media accounts, voice mails, or other digital assets of their deceased friends and relatives. Beth Teitell, *Preserving Voicemails Helps Modern Grieving Process*, Boston Globe, Nov. 20, 2013, http://tinyurl.com/l4tvbxa. For example, *David and Karen Williams v. Facebook, Inc.*, No. 0704-03971 (Multnomah Cnty. Cir. Ct. 2007), resulted in a Stipulated Order Permitting Access to Facebook.com Account Information, although the resulting information was unilaterally redacted by Facebook. A recent story to circulate is that of a teenage boy who, 10 years after his father died, discovered his “ghost” in a game they had played together when the boy was only six years old. Alex Lloyd, *Teenage Son Discovers His Deceased Father’s Ghost Car in Xbox Rally Game*, Yahoo! Autos (July 22, 2014), http://tinyurl.com/k5jxd3e.

Although the monetary value of social media accounts is generally small, access to the account may be priceless to family and friends. This is what motivated teenager Eric Rash’s parents, Ricky and Diane Rash, to become the driving force behind Virginia legislation that grants parents postmortem access to a minor’s Facebook account content. Tracy Sears, *Family, Lawmakers Push for Facebook Changes Following Son’s Suicide*, CBS 6 (Jan. 8, 2013), http://tinyurl.com/pwp63mp. With 7.5 million American children under the age of 13 using Facebook, a uniform approach to allow fiduciary access will save untold grief and litigation expense. Ray, *‘Til Death Do Us Part*, supra, at 588 (citing Somini Sengupta, *Update Urged on Children’s On-line Privacy*, N.Y. Times, Sept. 15, 2011, http://tinyurl.com/9b7w5lg).

In the well-known case of *In re Justin Ellsworth*, a U.S. Marine was killed in Iraq, and his family was denied access to his Yahoo e-mail account because of company policy. Justin Atwater, *Who Owns E-Mail? Do You Have the Right to Decide the Disposition of Your Private Digital Life?*, 2006 Utah L. Rev. 397, 399 (2006). Yahoo refused to give the e-mail password to the family as a result of its terms of service, which required the company not to disclose the private e-mail communications of its users. Id. at 401. The family filed suit against Yahoo, and in April 2005, a probate judge signed an order directing Yahoo! to provide the contents of the e-mail account used by Ellsworth. Id. Although Yahoo complied with the order, it maintained that its compliance was no way indicative of its stance on who holds legal title to the account information. Id. Yahoo’s compliance, it claimed, was a product of the court order, and it promised to defend its commitment to treat user e-mails as private and confidential. Id.

Rather than continue with costly litigation and varying legal interpretations that fail to provide consistency to businesses and individuals, UFADAA seeks to provide a dependable process throughout the United States.

Impediments to Fiduciary Access to Digital Assets

Passwords

Most on-line accounts are password protected, and generally the passwords can be reset or recovered only with access to the account holder’s e-mail account—if they can be reset or recovered at all.
**Inadequate Laws**

Only a minority of states have legislation dealing with fiduciary access to digital assets: Connecticut, Idaho, Indiana, Louisiana, Oklahoma, Rhode Island, Nevada, Virginia, and Delaware. H.B. 345, 2011-12 Leg., 129th Sess. (Ohio 2012) (signed into law on August 12, 2014, over on-line providers’ efforts to obtain a veto from the governor). Of those statutes, only the Delaware act is comprehensive and substantially similar to UFADAA, although numerous states have UFADAA in the legislative pipeline for consideration in 2015.

**Federal and State Computer Fraud and Abuse Acts**

Each state and Congress has enacted a Computer Fraud and Abuse Act (CFAA) that criminalizes (or at least, creates civil liability for) the unauthorized access of computer hardware and devices and the data stored thereon. The federal CFAA provides:

> (a) Whoever— . . . (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— . . . (C) information from any protected computer if the conduct involved an interstate or foreign communication; . . . shall be punished as provided in subsection (c) of this section.


Thus, the CFAA criminalizes “unauthorized access” to the Internet or a computer system or account because “obtaining information” could mean loading a web page, and a “protected computer” is defined not only as any computer connected to a government network but also as one used in interstate or foreign commerce. Because most Internet servers are not located in the same state as the web site’s user, using the Internet could involve obtaining information from a “protected computer” and thus implicate the CFAA. That is an unacceptable scenario for fiduciaries. Although “without authorization” is not defined, the term “exceeds authorized access” is defined at 18 U.S.C. § 1030(e)(6) in the CFAA to mean:

> [T]o access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.

This second prong, wherein a user who has access but exceeds his or her authority by accessing other files or information on the system, is designed to prohibit something nefarious: computer trespass. Although the state statutes vary in their coverage, they also typically prohibit “unauthorized access.”

Because the laws governing “access” to a computer or computer system or network call for authorization by the owner of that computer or system, they are directed at fraudulent activity such as malicious altering of computer systems and theft of services, and not authorized acts. See, e.g., 18 U.S.C. §§ 2701 and 1030.

Unfortunately, the fact that a fiduciary is “authorized” by the owner or state law to use a computer or to act for an account user may not be a bar to CFAA prosecution, even though it
should be. The analogy would be that using, or even hacking into, the computer is no more illegal than a fiduciary using a locksmith to get into a building owned by an incapacitated person, principal, or decedent. Accessing a hard drive, however, may be different from accessing the decedent’s, incapacitated person’s, or principal’s digital accounts or assets. By accessing another’s digital accounts or assets on-line, the fiduciary may be violating the account provider’s terms-of-service agreement (TOSA) and, in turn, the federal CFAA.

Very few people read TOSAs. Most of us open accounts and click through the TOSAs without a glance. To illustrate how easy it is unintentionally to violate a TOSA: an archived version of Google’s TOSA until recently prohibited minors who lacked contractual capacity from using its services. Google Terms of Service, http://tinyurl.com/mextubw (last visited Nov 25, 2014). The concern is that some federal prosecutors may use the CFAA to prosecute defendants based solely on violations of a web site’s TOSA. The Aaron Swartz case was a recent, highly publicized example of such prosecution. See Andrea Peterson, The Law Used to Prosecute Aaron Swartz Remains Unchanged a Year After His Death, Wash. Post, Jan. 11, 2014, http://tinyurl.com/otpk3d2. Aaron Swartz was a self-described Internet activist who committed suicide in 2013, while facing prosecution for downloading, without permission, 4.8 million academic articles from the JSTOR digital library system.

In 2006, a mother who created a fake “MySpace” profile in violation of MySpace’s TOSA, to bully a child who then committed suicide, was prosecuted and convicted solely under the CFAA. That is, no underlying state law violation applied to her conduct. Ultimately, the trial judge overturned her conviction, ruling that the conscious violation of a web site’s terms of service, alone, is not automatically a criminal violation of the CFAA. United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009).

Until Congress amends the CFAA, the scope and breadth of the CFAA’s reach remains unclear. Here is an excerpt from the written testimony of Richard W. Downing, deputy chief of the DOJ’s Computer Crime and Intellectual Property Section Criminal Division, before the House Judiciary Committee Subcommittee on Crime, Terrorism, and National Security, presented on November 15, 2011. This testimony evidences that the DOJ will continue to prosecute TOSA violations:

Finally, on behalf of the Department I want to address concerns regarding the scope of the CFAA in the context of the definition of “exceeds authorized access.” In short, the statute permits the government to charge a person with violating the CFAA when that person has exceeded his access by violating the access rules put in place by the computer owner and then commits fraud or obtains information. Some have argued that this can lead to prosecutions based upon “mere” violations of website terms of service or use policies. As a result, some have argued that the definition of “exceeds authorized access” in the CFAA should be restricted to disallow prosecutions based upon a violation of contractual agreements with an employer or service provider. We appreciate this view, but we are concerned that restricting the statute in this way would make it difficult or impossible to deter and address serious insider threats through prosecution.

Encryption

Access to the computer does not automatically grant the fiduciary access to the data stored on the computer’s hard drive if the data are encrypted. One often cited example of this was Leonard Bernstein, who died in 1990, leaving the manuscript for his memoir titled “Blue Ink” on his computer in a password protected file. To this day, no one has been able to break the password and access the document. Helen Gunnarsson, *Plan for Administering Your Digital Estate*, 99 Ill. B.J. 71 (2011).

Copyright, Commercial Privacy, and Data Protection Statutes

Other bodies of law might impede a fiduciary from downloading or distributing another person’s digital files: such action may violate copyright law, the limited common law of privacy, trade secret law, and federal and state personal data protection statutes. For example, Massachusetts has a data security statute that requires encryption of personal information “owned or licensed [held by permission]” by any person. See 201 Mass. Code Regs. § 17.00 (2010) (generally effective March 1, 2010, which requires businesses to encrypt sensitive personal information on Massachusetts residents that is stored on portable devices such as PDAs and laptops or on storage media such as memory sticks and DVDs). According to the National Conference of State Legislatures, 46 states have enacted a data breach or privacy law of some kind.

The Stored Communications Act

The Fourth Amendment to the U.S. Constitution provides citizens with a strong expectation of privacy in their homes: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[.]” As a result, the government cannot normally search our homes without first showing probable cause and obtaining a search warrant authorizing a search.

When we use a computer network, we may have the same personal expectation of privacy, but, of course, the network is not located in our homes. Addressing this issue, Congress enacted the Stored Communications Act (SCA) in 1986, as a part of the Electronic Communications Privacy Act (ECPA). See generally 18 U.S.C. §§ 2701–2711; see also Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004). “The SCA is notoriously complicated and confusing, and its application to social networking sites has only further muddied the waters.” Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 Wash. & Lee L. Rev. 1259, 1264 (2012). “Despite vast technological advancement since the SCA’s passage, Congress has yet to update the SCA to conform to modern day innovations related to e-mail and cell phones, among other things.” Id.

The way the privacy protections of the Stored Communications Act work is to prohibit certain providers of public communications services from disclosing the contents of the user’s communications to a government or nongovernment entity (different rules apply to each), except under limited circumstances that are akin to the “warrant” required under the Fourth Amendment. So, if the provider of the electronic communications service provides it only to
employees or students, and not to the general public, that provider is not subject to the SCA and cannot use its provisions as a shield against a fiduciary’s request or law enforcement demands for copies of communications or access to an account. But it is crucial to understand that the SCA applies different rules to government/law enforcement entities requesting information and all others, such as fiduciaries. Under the SCA, law enforcement officials can force or compel the provider who is otherwise covered and subject to the SCA to divulge the contents of an account. A fiduciary, however, cannot compel the provider to divulge the same information. Indeed, Google recently took the position, unsuccessfully, that the SCA confers “a blanket exemption or immunity on service providers against compulsory civil discovery process.” Negro v. Navalimpianti USA, Inc., 179 Cal. Rptr. 3d 215, 230 (Ct. App. 2014). That California court failed to follow such a restricted reading of the SCA: “The Act cannot be so construed.” Id.

A public communications provider can voluntarily disclose communications to a fiduciary, but only if an exception to the SCA’s prohibition against disclosure applies. 18 U.S.C. § 2702(b). The relevant exception for fiduciaries permits service providers to disclose communications with the “lawful consent” of “the originator” or an addressee or intended recipient of such communication, or the subscriber. 18 U.S.C. § 2702(b)(3). To give providers reassurance that a fiduciary can have such “lawful consent,” underlying state law or a court order should expressly provide that the fiduciary requesting the contents of SCA protected material has the user’s lawful consent. That is why Facebook essentially asked one court, in a memorandum supporting Facebook’s motion to quash a civil subpoena for information contained in a deceased user’s profile and account, to alternatively hold that the fiduciary had lawful consent and to order Facebook to disclose the requested content. Facebook, Inc.’s Motion to Quash Subpoena in Civil Case, No. C 12-80171 LHK (N.D. Cal. Aug. 6, 2012). The court granted Facebook’s motion and quashed the subpoena. In re Request for Order Requiring Facebook, Inc., to Produce Documents and Things, No. C 1280171 LHK (N.D. Cal. Sept. 20, 2012). A more recent ruling, however, minimized extraneous statements in that case: “The court’s remarks on this point may have been dictum.” Negro, 179 Cal. Rptr. 3d at 232 n.6.

A federal jury in Massachusetts awarded a plaintiff significant monetary damages in a civil action brought under the SCA recently. The defendant had been given the plaintiff’s e-mail account password so she could access it to read consultation reports when the two parties practiced medicine together. When the defendant left the practice and a business dispute arose, the defendant used the plaintiff’s unchanged password to access the account for reasons connected to the business dispute. The plaintiff sued, alleging her later access was unauthorized under the SCA. Despite very thin testimony to support the damage claim, the jury awarded the plaintiff $450,000 for the unauthorized intrusion. Jury Verdict Form, at 13, Cheng v. Romo, No. 11-cv-10007-DJC, 2013 WL 2245312 (D. Mass. Apr. 29, 2013); Cheng v. Romo, No. 11-1007-DJC, 2012 WL 6021369, at *13 (D. Mass. Nov. 28, 2012).

Providers are allowed to divulge noncontent information, such as the user’s name, address, connection records, IP address, and account information because the SCA only prohibits the disclosure of the contents of communications. Providers are still balking, however, at granting executors access to the content of decedents’ e-mail accounts. Recently, Yahoo! refused to accept a co-administrator’s authority to access his deceased brother’s e-mails, even though the surviving brother had opened and had shared access to the account but had forgotten the
password. Ajemian v. Yahoo!, Inc., 987 N.E.2d 604, 613 (Mass. App. Ct. 2013). Yahoo! attempted to dismiss the Massachusetts declaratory action based on the California forum selection provision in its TOSA and claimed that the e-mails were not property of the Massachusetts estate, among other arguments. The appeals court refused to enforce the adhesive TOSA provisions but remanded the case to the probate court to determine whether or not the e-mails were an asset of the estate and whether or not the SCA barred Yahoo! from disclosing them. The court’s opinion differentiated between “clickwrap” agreements (requiring the user to click an “I agree” box) and “browsewrap” agreements in which the terms are simply posted, but the user need not confirm having read them. The court concluded that without evidence that the account holder agreed to the TOSA, the TOSA was not enforceable against anyone, especially not against the estate’s co-administrators, who were not parties to it.

Private social media account contents with photos, videos, or posts may all be “communications” protected by the SCA. See Burshnic, Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites, supra. UFADAA clarifies that fiduciaries are “authorized users” with “consent” comporting with the federal laws such that on-line providers and fiduciaries will not risk running afoul of federal laws when fiduciaries are provided access to on-line accounts and information.

The Terms of Service Agreements

The account provider’s TOSAs are frequently silent as to fiduciary access or postmortem options, or they may prohibit postmortem transfer altogether. For example, Yahoo’s policy specifies:

We know that dealing with the loss of a relative is very difficult. To protect the privacy of your loved one, it is our policy to honor the initial agreement that they made with us, even in the event of their passing.

At the time of registration, all account holders agree to the Yahoo Terms (TOS). Pursuant to the TOS, neither the Yahoo account nor any of the content therein are transferable, even when the account owner is deceased. As a result, Yahoo cannot provide passwords or access to deceased users’ accounts, including account content such as email.

Yahoo does have a process in place to request that your loved one’s account be closed, billing and premium services suspended, and any contents permanently deleted for privacy.

Options Available When a Yahoo Account Owner Passes Away, Yahoo! Help, http://tinyurl.com/q76cvg8 (last visited Nov. 25, 2014). Facebook’s policy on postmortem account use and access has been widely publicized. Unlike Google, Facebook has not updated its policies on postmortem access. Essentially, Facebook will allow a personal representative or family member to obtain content with a court order via “Special Request.” See How Do I Submit a Special Request for a Deceased Person’s Account on the Site?, Facebook, http://tinyurl.com/k2lدب6 (last visited Nov. 25, 2014) (once the account is “memorialized,” Facebook will not allow anyone except the user (who presumably would then have to prove that the user has not actually died, as reported) to log into it. It will allow verified family members to
request that the account be removed from Facebook). Tucker Bounds, a spokesman for Facebook, has stated, however: “We will provide the estate of the deceased with a download of the accounts’ data if prior consent is obtained from or decreed by the deceased, or mandated by law.” Alissa Skelton, Facebook After Death: What Should the Law Say?, Mashable (Jan. 26, 2012), http://tinyurl.com/7r89yn9. With that admission, UFADAA actually supports Facebook’s stated policy.

Apple’s iTunes terms-of-use grants the account holder a license to download and use/listen to digital music files, but expressly prohibits their sale or transfer. This may or may not allow the user to bequeath the content or actual music files—the terms-of-use do not mention death. See Terms and Conditions, Apple, http://tinyurl.com/p69flak (last visited Nov. 25, 2014).

Amazon’s Kindle books, however, can indeed be willed, so it may be that on-line providers will begin to acknowledge the consumer demand for more choices. Katy Steinmetz, From Here to Eternity: What Happens to Your Virtual Things When You’re Gone?, Time, Feb. 11, 2013. “Shoppers shelled out an estimated $4.5 billion last year for e-books and billions more for music, movies and other stuff that exists only on a computer or in the cloud.” Id.

With court opinions not always in alignment as to the enforceability of clickwrap or shrinkwrap on-line providers’ TOSAs, “the enforceability of agreements that require a mere ‘click’ to assent may not be as uniformly enforceable as large social media companies would have their users believe.” Ray, ‘Til Death Do Us Part, supra, at 601.

UFADAA authorizes fiduciaries to fulfill their responsibilities for on-line assets. This is not a new legal concept but rather a natural extension of the responsibilities a fiduciary has in connection with on-line assets. But without the statutory changes, the on-line providers often hold all of the power, including the power to hit the delete button and destroy irreplaceable financial or personal information.

A fiduciary is legally obligated to marshal assets and distribute, under the decedent’s stated intent. As more and more people move more and more assets and information on-line, how can a fiduciary get the necessary information? If a fiduciary goes on-line and uses a decedent’s password, then that is a cybercrime in most states and under federal law for making a fraudulent representation to the end user.

A fiduciary must have a predictable way to access and manage on-line assets. That is what UFADDA does. It does not create new law; it allows fiduciaries to comply with their existing responsibilities. Otherwise, the fiduciaries are in the impossible position of being ordered to marshal on-line assets but not having the authority to do so.

**Bridging the Gap to Confirm Fiduciaries Are Authorized Users with Consent to Access**

Who do you want making decisions for your estate: your fiduciary or the on-line providers? At least 27 states have proposed UFADAA legislation in 2015, in many instances supported by state-sponsored organizations. This should not be a controversial topic. The only controversy is
that on-line providers have a lot of money to hire lobbyists to cry that the sky is falling, but it is not.

An existing body of law governs what fiduciaries can and cannot do, but to do their jobs, they must have on-line access.

Business owners need this law. Let’s look at the small- to medium-sized business—which is what the United States of America is founded on—and what happens when the owner becomes incapacitated or dies? Most laypeople believe that someone will have access to their personal and business digital accounts to handle their affairs. But that is not true.

**UFADAA Approach in General**

UFADAA aims to resolve the impediments to fiduciary access to digital assets. UFADAA defines digital assets, provides default rules, defers to the intent of account holders and privacy desires, and encourages custodian compliance. It was drafted with the assistance of observers from several state bar committees and from NAELA, ACTEC, Facebook, Google, Yahoo, NetChoice, Microsoft, The Verge, Northern Trust, the American Bankers’ Association, and representatives from the gaming industry. Although some Internet industry observers objected to some UFADAA provisions, the final version of the act differentiates between electronic mail content that is protected by the SCA and other content, as they had requested.

**Key Concepts and Definitions**

UFADAA covers personal representatives, conservators, agents acting under powers of attorney, and trustees. By defining the fiduciary as an authorized user, the act gives the fiduciary the authorization to access digital files under the first section (18 U.S.C. § 2701) of the SCA as well as under the CFAA, and it gives the fiduciary “the lawful consent” of the originator/subscriber so that the provider can voluntarily disclose the files under the second relevant provision of the SCA (18 U.S.C. § 2702). Moreover, this language should be adequate to avoid liability under state unauthorized access laws.

UFADAA grants fiduciaries access to digital assets limited to what is necessary to carry out their fiduciary duties; it is not personal access and does not allow a fiduciary to maintain or continue social media accounts by “impersonating” the account holder for whom the fiduciary is acting.

UFADAA § 2(1) defines an “account holder” as a person who has entered into a terms-of-service agreement with a custodian or a fiduciary for such a person. UFADAA § 2(8) defines a custodian as “a person that carries, maintains, processes, receives or stores a digital asset of an account holder.” (Elsewhere, UFADAA § 3(b) specifies that an employer is not a custodian under most circumstances.) UFADAA § 2(3) defines “carries” as engaging in the transmission of electronic communications, which is based on language in 47 U.S.C. § 1001(8).

UFADAA § 2(9) defines “digital asset” as a record that is electronic, not including an underlying asset or liability unless the asset or liability is itself a record that is electronic. This includes both the catalogue of electronic communications and the content of electronic communications, but it
would exclude securities or currency. For example, consider an on-line commodities account for purchasing gold bullion. The digital assets covered by UFADAA are the records concerning the account, not the gold bullion itself.

UFADAA § 2(6) defines “content of an electronic communication” (EC) as information concerning the substance or meaning of the communication that has been sent or received by an account holder, that is in electronic storage by a custodian “covered” by the SCA, and that is not readily accessible to the public and is therefore “protected” by the SCA. So, such content is defined narrowly in reference to the SCA. Other EC content is covered not by this definition but instead by the broader definition of a digital asset. UFADAA § 2(11) defines electronic communication as it is defined in 18 U.S.C. § 2510(12), which is, essentially, a transfer of data or signals electronically. Securities held in street name or money in a bank are not digital assets; UFADAA reinforces the fiduciary’s right to access all relevant electronic communications and the on-line account that provides evidence of ownership.

**Personal Representatives’ Access**

UFADAA § 4 is devoted to access by personal representatives, which is available by default unless the decedent prevented access in a TOSA election that complies with UFADAA § 8(b) or in a will, or a court otherwise prohibits access. In deference to custodians’ unease as to the availability of fiduciary authority under SCA, personal representatives have access to electronic communications content only if disclosure is permitted under federal law.

**Conservator or Guardian Access**

UFADAA § 5 permits a court to authorize conservator access to digital assets after the opportunity for a hearing. The protected person’s privacy is protected by default. Disclosure of EC content may be ordered only if permitted under federal law. State law typically requires the court to consider the protected person’s intent, best interests, and personal values. Social media companies object to ongoing use of an account, as opposed to limited access, which is why the act speaks of “access” and not management.

**Access by Agents Acting Under Powers of Attorney**

UFADAA § 6 provides that unless prohibited by the principal, an agent has access to most of the principal’s digital assets and the principal’s catalogue of electronic communications. The act, however, does not give an agent default authority over electronic communications content, so this authority is akin to gifting in that the principal must expressly include the authority to grant access. Although debate about this policy was lengthy on the floor of the annual meeting, ultimately the Uniform Law Commission voted to track the SCA, which requires the account holder’s lawful consent. For that reason, UFADAA makes access to EC content by an agent a “hot” power—something that must be identified specifically in the power of attorney document.
Access by Trustees

UFADA § 7 provides that trustees who are original account holders can access all digital assets held in the trust. There should be no question that when the trustee is the original account holder, it will have full access to all digital assets. For assets that are transferred by the settlor or otherwise, a trustee becomes the successor account holder of the digital assets. Although the designation or transfer of the legal title should supply the necessary “lawful consent” under federal law, UFADA § 7(b) distinguishes between access to EC content and the catalogue when the trustee is not the original account holder, just to be safe.

In all cases, the settlor is free to prevent trustee access to digital assets by language in the trust instrument or by a TOSA election that complies with UFADA § 8(b), or a court can prohibit access, satisfying privacy concerns.

UFADA does not contain provisions facilitating the transfer of digital assets into a trust. That transfer would be accomplished by the settlor while alive and capable, the settlor’s agent, or a personal representative. Underlying trust documents or default trust law generally supplies the allocation of responsibilities among trustees. Therefore, drafters should consider access to digital assets when drafting trustee powers provisions.

Fiduciary Authority

UFADA § 8 specifies the nature, extent, and limitation of the fiduciary’s authority over digital assets. UFADA § 8(a)(1) establishes that the fiduciary is authorized to exercise control over digital assets subject to the TOSA and applicable laws, such as copyright, and that the fiduciary may act only to the extent of the account holder’s authority and the fiduciary’s powers. UFADA § 8(a)(2) says that the fiduciary has the account holder’s lawful consent under applicable electronic privacy laws. UFADA § 8(a)(3) further specifies that the fiduciary is an authorized user under any applicable CFAA.

The fiduciary has the same authority as the account holder except when, under UFADA § 8(b), the account holder has explicitly opted out of fiduciary access. This renders a boilerplate TOSA provision limiting fiduciary access as void against public policy. The TOSA can allow an account holder to prevent access, but it must be an affirmative election. The drafting committee felt this was absolutely necessary, given the reality of widespread user ignorance of TOSA provisions. See Londoners Give Up Eldest Children in Public Wi-Fi Security Horror Show, The Guardian, http://tinyurl.com/ng8379o (last visited Nov. 25, 2014) (reporting on Londoners connecting to free public Wi-Fi who were asked to approve terms and conditions that included a “Herod clause” promising the free Wi-Fi, but only if “the recipient agreed to assign their first born child to us for the duration of eternity.” Six people signed up).

UFADA § 8(b)(2) reinforces the “stepping into the shoes” nature of fiduciary authority by indicating that the fiduciary’s access, by itself, will not violate a TOSA provision prohibiting third-party access. This will prevent prosecutions based solely on a fiduciary’s access. Subsection (c) supports the importance of fiduciary access by providing that any choice of law governing the effect of a TOSA that prevents fiduciary access is unenforceable. Subsection (d)
clarifies that the fiduciary is authorized to access digital assets stored on devices, such as computers or smartphones, avoiding violations of state or federal laws on unauthorized computer access.

**Compliance and Immunity**

UFADAA § 9 provides that if a fiduciary has access under UFADAA and substantiates his or her authority as specified, a custodian must comply with the fiduciary’s request for access, control, or a copy of the digital asset.

UFADAA thereby mandates what the SCA merely permits if the request is for EC content. In exchange, UFADAA § 10 immunizes a custodian who complies with the request.

**Applicability**

UFADAA § 3 provides that the act is applicable to the actions of all fiduciaries regardless of the date their authority was granted by a court or in an instrument. UFADAA § 3(b) provides that the act does not apply to digital assets of an employer used by an employee in the ordinary course of the employer’s business. This language is intended to preclude fiduciary access to employer-provided e-mail systems and employer data. It would allow fiduciaries of the employees of custodians who have personal accounts (with the employer custodian) that are not used for business to access the personal accounts. So, for example, a Yahoo! employee’s fiduciary would not have access to the employee’s business e-mail or other accounts but potentially could access a personal Yahoo! account.

**The Temperature Increases as On-line Providers Gather the Lobbyists**

Although five states had already passed legislation authorizing fiduciary access to digital assets when the ULC began its research on this important issue, and the on-line providers have been intimately involved in the ULC conversation, now that UFADAA is a viable legislative option for states to move forward, certain lobbyists for on-line providers have begun a full court press to scare state legislators away from the topic.

Only a few behemoth businesses do not like this law. And when you are Goliath, certainly your viewpoint is different from David’s. Michael Scherer, *Hacking Politics*, Time, June 17, 2013 (“In 2012, Google alone spent $23 million on direct corporate lobbying in D.C., more than defense contractors like Boeing, drug firms like Pfizer and oil companies like ExxonMobil”). When you have companies like Yahoo that have TOSAs allowing them to hit the delete button when the account holder dies, then yes, they do not like this law. But how is the fiduciary going to perform his job when the very assets he is supposed to marshal are within that account?

The worldview from some on-line providers is that they cannot and will not provide any on-line information without a criminal warrant; they appear to have no regard for the civil courts and scoff at the long-standing notion that a duly appointed fiduciary steps into the shoes of the decedent.
In a slight variation on the claim of a blanket exemption, Google contends that the language of the Act makes the consent exception “permissive” and the provider’s disclosure under it “voluntary.” Thus the Act, in Google’s view, “allows, but does not require, disclosure by an electronic communications service provider,” so that “Google may not be compelled by an order issued in a civil proceeding to disclose content, even with the user’s consent.” According to Google, the “text and title of the SCA could not be clearer” on this point.

Negro, 179 Cal. Rptr. 3d at 231. The California court did not agree with Google’s position: “This reading of the Act, however, does not survive scrutiny.” Id.

The legal reality that fiduciaries are a special group is a concept banks already understand. From a banking perspective, UFADAA is not a new and sexy law; banks already understand that when a decedent dies, the personal representative steps into the shoes of the decedent and will be allowed access to accounts or safe deposit boxes. On-line accounts are simply a different storage box. Trust officers from banks and other corporate fiduciaries support UFADAA because it provides certainty.

If UFADAA legislation does not move forward, it will be for one reason only—well-paid lobbyists’ fear tactics are scaring people from bringing the law up to date so that fiduciaries can properly perform their legal obligations. The positive effect UFADAA will have is apparent for fiduciaries trying to do their jobs, any business conducting business on-line or an individual with on-line accounts who becomes incapacitated or dies, and banks and trust companies that seek straightforward laws as guidance. All need certainty in the law. If state legislators back down because a few well-paid lobbyists scream that the sky is falling, then these constituencies are left in an ethical dilemma when working with a diverse group of clients: are attorneys supposed to advise them to commit a cybercrime by accessing an on-line account in the current confusion? How do we help our clients when the law has a gaping hole in it? The law must change to catch up with technology.

This is not a privacy issue. Fiduciaries routinely deal with private documents and issues. A well-established body of law governs fiduciaries in the performance of their responsibilities—the duty of loyalty, the duty to administer prudently, and the duty of confidentiality. Just because a fiduciary has authority under UFADAA to access on-line accounts or information does not require the fiduciary to do so in all situations, nor does it require the fiduciary to broadcast the information to the world. In fact, a fiduciary would subject himself to claims of breach of his fiduciary duty if he went rogue with on-line access. Laws are already in place that govern a fiduciary’s proper performance once he has access to on-line assets and information. UFADAA is necessary to open the door so that fiduciaries can perform their jobs appropriately.

This is an important policy issue: a fiduciary should have access on behalf of a decedent or protected person even though the access may not comply with a TOSA. Banks have safe deposit boxes, yet a personal representative has the authority to access the safe deposit box when a person dies, regardless of the contract. On-line accounts are just information stored in a different box—an electronic box. Indeed, it is interesting to note that, although fiduciaries have the right to complete access to federal U.S. mail addressed to a decedent or protected person, some on-line companies take the position that fiduciaries do not have the same rights to digital information.
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

and assets. A fiduciary has always had access to personal and perhaps sensitive information, including finding a long lost box of letters to a secret lover or incriminating photos or documents in the far reaches of a bottom drawer. The challenge of how a fiduciary handles private or sensitive information is not a new challenge.

Since 2010, some states have enacted laws addressing digital assets or accounts: Connecticut, Idaho, Indiana, Oklahoma, and Rhode Island. To date, none of these laws has been overturned, despite the new focus by on-line providers on arguing that federal law prohibits production of on-line information.

Conclusion: Why Your State Should Adopt UFADAA

UFADAA modernizes fiduciary law for the Internet age. Nearly everyone today has digital assets, such as documents, photographs, e-mails, and social media accounts. Digital assets have both monetary and sentimental value. But Internet service agreements, passwords that can be reset only through the account holder’s e-mail, and federal and state privacy laws that do not contemplate that the account holder’s death or incapacity may prevent fiduciaries from gaining access to these valuable assets. UFADAA solves the problem by ensuring that fiduciaries can access, delete, preserve, and distribute digital assets as appropriate.

- UFADAA gives account holders control. UFADAA allows account holders to specify whether their digital assets should be preserved, distributed to heirs, or destroyed.
- UFADAA treats digital assets like all other assets. If a fiduciary has authority to inventory and dispose of all of a person’s documents, it should not matter whether those documents are printed on paper, stored on a personal computer, or stored in the cloud. UFADAA provides a fiduciary with access to digital property.
- UFADAA provides rules for four common types of fiduciaries. The executor of a decedent’s estate has responsibilities different from those of an agent under a living person’s power of attorney. UFADAA provides appropriate default rules governing access for executors, agents, conservators, and trustees.
- UFADAA protects custodians and copyright holders. Under UFADAA, fiduciaries must provide proof of their authority in the form of a certified document. Custodians of digital assets that comply with a fiduciary’s apparently authorized request for access are immune from liability. A fiduciary’s authority over digital assets is limited by federal law, including the Copyright Act and the Electronic Communications Privacy Act.
- UFADAA provides efficient uniformity for all concerned. Digital assets travel across state lines instantaneously. In our modern society, people relocate more often than ever. Because state law governs fiduciaries, a uniform law ensures that, regardless of the state, fiduciaries will have equal access to digital assets and custodians will benefit from uniform regulation.

Contact ULC Legislative Counsel, Benjamin Orzeske, with any questions at borzeske@uniformlaws.org.

UFADAA updates state fiduciary law for the Internet age. When a person dies or loses the capacity to manage his or her affairs, a fiduciary receives legal authority to manage or distribute
the person’s property as appropriate. Most people now own a variety of digital assets, including photographs, documents, social media accounts, web sites, and more. Access to digital assets is often limited by custodians through restrictive terms-of-service agreements. UFADAA ensures that fiduciaries have the access they need to carry out their duties in accordance with the account holder’s estate plan, if there is one, otherwise in the account holder’s best interests.

UFADAA provides a predictable manner by which a fiduciary, consistent with well-established fiduciary law, can deal with on-line accounts and assets. UFADAA does not create new law but rather allows fiduciaries and on-line providers to comply with the current law without inadvertent exposure to federal laws. Otherwise, fiduciaries are in the impossible position of being ordered to marshal and distribute assets without the ability to gain access. UFADAA avoids such chaos.
Planning for Fiduciary Access to Digital Assets

Probate & Property Magazine: Volume 29 No. 05 (Reprinted with permission of author)

Victoria Blachly

In the July/August issue of Probate & Property, Uniform Fiduciary Access to Digital Assets Act: What UFADAA Know discussed the Uniform Law Commission’s more than two-year process to mend a large gap that prohibits fiduciaries from doing their legally mandated job. In this article, the author provides tips for estate planning with digital assets.

In the July/August issue of Probate & Property, I discussed the Uniform Law Commission’s effort to mend a large gap that prohibits fiduciaries from doing their legally mandated job. See generally Uniform Fiduciary Access to Digital Assets Act (UFADAA) (2014), available at http://tinyurl.com/p7oshx1. In this article, I will provide tips for estate planning with digital assets.

Collectively, a person’s digital property and electronic communications are referred to as “digital assets,” and the companies that store those assets on their servers are called “custodians.” Access to digital assets is usually governed by a restrictive terms-of-service agreement (TOSA) provided by the custodian. This creates problems when account holders die or otherwise lose the ability to manage their own digital assets. Although no definition of digital assets is universally accepted, UFADAA defines them as electronic records, not including an underlying asset or liability unless the asset or liability is itself a record that is electronic. All digital assets, however defined, are accessed by a tangible device, such as a computer, smartphone, tablet, or a server. Jamie P. Hopkins, Afterlife in the Cloud: Managing a Digital Estate, 5 Hastings Sci. & Tech. L.J. 210, 212 (2013).

Planning for Fiduciary Access to Digital Assets

Education is vital to alert businesses and individuals to the importance of proactively managing on-line accounts and assets. With the adoption of UFADAA, if a person fails to plan, then the court-appointed fiduciary that manages the person’s tangible assets can manage the person’s digital assets, distribute those assets to heirs, or dispose of them as appropriate. In the meantime, some custodians of digital assets provide an on-line planning option by which account holders can choose to delete or preserve their digital assets after some period of inactivity. But without certainty, the need to educate clients on how to plan for a fiduciary to have access to their digital assets is paramount.

Digital Asset Awareness

At a minimum, clients need to be advised to develop an inventory of digital assets, including a list of how and where they are held, along with user names, passwords, and password “prompts.” Sarah Kellogg, Managing Your Digital Afterlife, Wash. Law. (Jan. 2013), available at

To prevent identity theft, security experts advise using different passwords for all web sites, changing them constantly, and using random combinations of numbers and letters. Another option is a dedicated password memorization program installed on the client’s computer that can memorize all of the client’s passwords for her, requiring her to learn only one master password for the master program. The first option requires a level of dedication many of us do not possess, yet the second option allows for the proverbial “keys to the kingdom” to be located in one location. Neither option is perfect.

**E-Mail Correspondence**


If a deceased leaves behind a computer hard drive containing copies of email messages, these messages would pass to the next of kin just as would a shoebox full of old letters. Heirs might similarly inherit previously printed copies of email messages. However, the copyright in these messages would pass separately and independently to the heirs either [by will or intestacy].

Id. at 299. Just like a paper letter, the author who owns the copyright in a sent message cannot compel the recipient to return it but can prevent the recipient from reproducing, distributing, or displaying it. Id. E-mails, however, are unlike traditional letters in several ways. Compared to paper letters, lost copies might be easily located and retrieved from an e-mail service provider. Access to e-mails may be important not because they have literary value, but because a decedent’s e-mail account contains the information necessary to continue a business or collect other assets. E-mails concerning financial and business accounts can be quite time-sensitive.

**Estate Planning Documents Should Address Digital Assets Properly**

Wills, trusts, and powers of attorney have been around for centuries. In appointing an executor, trustee, or agent under a power of attorney, the testator appoints a representative that she trusts to take control of her assets and to follow her legal instructions. Whether dealing with digital assets or an office building, the testator should appoint individuals in these roles that are both trustworthy and competent to carry out these instructions.
Some digital assets have value, at least while the owner is alive and can access them. So, the estate and trust attorney’s natural reaction is to assume that all digital assets behave and are legally treated just like their brick-and-mortar counterparts. Not all digital assets are transferable on death, however. Depending on the nature of the digital asset and the TOSA, then, the service provider may or may not recognize a traditional will or trust as validly transferring either access to, or ownership of, the account.

Not so long ago it was much more difficult for one person to give another access to bank and financial accounts during incapacity. At a minimum, a written, notarized durable power of attorney or joint/agency bank or trust account was required. Today, all that might be required is an on-line password. Some clients will wish to give their agents authority over digital accounts, although it is still unclear to what extent financial and on-line institutions will honor that authority, and policies differ.

It is important not only to include provisions for the disposition of digital assets with monetary or sentimental value, but also to provide for the destruction or securing of digital assets the client wants kept secret. Further, fiduciary powers provisions must cover digital assets, and if they are to be destroyed or accounts terminated, that direction should be accompanied by a corresponding exculpation provision. Until the federal privacy and fraud and abuse laws expressly recognize fiduciary authority, civil or criminal liability may be associated with any third-party access to digital accounts, as discussed above. See Lior Jacob Strahilevitz, *The Right to Destroy*, 114 Yale L.J. 781 (2005), available at http://tinyurl.com/mucjola. (Note that fiduciary destruction of an otherwise valuable asset, even at the decedent’s direction, may be unwise, as the fiduciary’s duties to the beneficiary may be paramount.)

In April 2013, Google introduced an option called “Inactive Account Manager” to allow users to determine, within preset options, what will happen to their Google accounts after a predetermined period of inactivity. Users can set the time period of inactivity that triggers a Google response, and Google also will alert the user by text and e-mail one month before deleting the account. Users may have Google notify up to 10 “beneficiaries” that the account will be closed, before Google deletes it. After the recipients receive that notice, those designated “beneficiaries” can download the user’s Google content (such as gmail, photos, or YouTube videos and blogs). Or, the user can simply instruct Google to delete all account content. See About Inactive Account Manager, Google, http://tinyurl.com/16mqpkz (last visited Nov. 25, 2014). Although this feature will not assist with postmortem access if it is not used by the deceased account holder, or if the designated “beneficiary” is unavailable, incapable, or dead, it is a step forward.

A virtual asset instruction letter, or “VAIL,” lists all of the testator’s on-line accounts and assets and provides web addresses, user names, and passwords to give the testator’s designated representative the ability to identify and access these accounts. Michael Walker & Victoria D. Blachly, *Virtual Assets*, ST003 A.L.I.-A.B.A. 175, 177 (2011), http://files.ali-cle.org/thumbs/datastorage/skoobesruoc/pdf/CT003_chapter_07_thumb.pdf; VAIL 7-steps created by Jeffrey M. Cheyne. Think of VAIL as a verb, an action, and more than one project that fits everyone’s needs:
1. Identify each Internet account that you have and determine how each company handles an account when the account holder dies.

2. Determine which accounts you want your representative to maintain and have access to, and prepare a written and electronic file list of those accounts with their passwords.

3. Determine which accounts you wish to have deleted and provide the necessary written instructions to do so.

4. Consider saving the account and access information on a CD or memory stick and store it in a safe place. Give your representative instructions about how to access this information. Don’t forget to update it as passwords change.

5. If you have a collection of pictures or other memorabilia that are being stored on the Internet, consider making a backup of that information to a disk drive or CD that you control. Store this information in a safe place, and provide your personal representative with instructions on how to obtain that information.

6. Upgrade your power of attorney, trust, and will to include provisions authorizing your agent to access your e-mails and other electronic data.

7. If someone other than your personal representative is being designated to handle your electronic data, then those individuals should be named in your will or other estate planning documents.

The VAIL should be placed in a safe location, such as a safe deposit box, that can be accessed only by the testator’s legal representative. In addition to a written list, consider saving the VAIL to a flash memory drive or CD, which can make the testator’s representative’s access to these accounts more efficient. For assets such as e-mail accounts, the testator’s VAIL can instruct his representative to delete the account after a period of time. Some accounts may simply terminate after a certain period of inactivity. Although a VAIL may seem time-consuming or almost insurmountable, its importance is directly related to the complexity or importance of one’s online accounts or information.

Gaining access to another’s on-line accounts is often more troublesome in cases of incapacitation. One reason for this is the fact that the records may be needed to access assets to meet expenses, which continue while a person is disabled but which generally end at death. Informal measures, such as giving a password to a child so that he or she can pay the bills of an ill parent can be problematic. If, for example, a sibling accuses that child of misusing funds, the child may need the parent’s authorization and instructions to defend herself. Deborah L. Jacobs, *When Others Need the Keys to Your Online Kingdom*, N.Y. Times (May 20, 2009), available at http://tinyurl.com/mlmzw9a.

Some recommend preparing a durable power of attorney that authorizes another individual to act as an agent and handle finances to avoid these problems. Id. Absent UFADAA’s adoption, however, a power of attorney alone may not be sufficient in the electronic world. Id. Bills paid on-line, automatically charged to a credit card or debit card account, can nevertheless be hard to identify and audit. Id. A VAIL provides the necessary information to a trusted fiduciary to perform these duties.
Estate Administration of Digital Assets

Checklist of Basic Steps

Although much of this checklist assumes that the fiduciary is granted full access, control, and authority over the decedent’s accounts, and is thereby deemed an “authorized user” who steps into the decedent’s shoes for all purposes, here are some basic steps fiduciaries should consider.

1. Get technical help if necessary. “In-house technicians may be able to access the hard drive and copy its contents to a DVD. They may first ask to see documentation such as a death certificate, certificate of appointment or the decedent’s proof of ownership.” Colin Korzec & Ethan A. Mc-Kittrick, Estate Administration in Cyberspace, Tr. & Est., n.12 (Sept. 2011) (“Telephone conversation with Best Buy technician, Boston, May 2, 2011. Actual policy may differ by store or company”). Consider retaining a service that can perform a comprehensive Internet search for accounts affiliated with the decedent. See generally WebCease Home Page, www.webcease.com (last visited Nov. 25, 2014) (“WebCease identifies active online accounts for the deceased and instructs on the different options for retrieval, closure or memorialization in accordance with the policies of each site”).

2. Consolidate virtual assets to as few “platforms” as possible by having multiple e-mail accounts set to forward to a single e-mail account.

3. Obtain statements or data of the prior 12 months of the decedent’s important financial accounts.

4. Consider notifying the individuals in the decedent’s e-mail contact list and other social media contacts.

5. Change passwords to those that the fiduciary can control.

6. Keep all accounts open for some period of time to make sure all relevant or valuable information has been saved and all vendors or other business contacts have been appropriately notified, and so all payables can be paid and accounts receivable have been collected.

7. Remove all private and personal data from on-line shopping accounts or close them as soon as reasonably possible.

8. Plan on archiving important electronic data for the full duration of the relevant statutes of limitations.

Walker & Blachly, Virtual Assets, supra, at 177.

Without state statutes or estate documents that treat digital accounts and assets any differently from other assets for purposes of inheritance or trust law, fiduciaries need to be aware of digital assets and who is controlling them to determine whether their disposition comports with the decedent’s estate plan.

Effectuating a Decedent’s Intent

Some decedents may have wanted to prevent postmortem access to, or publication of, the content of their digital accounts. Some will, no doubt, figure out how to block family or fiduciary access...
by using an account manager feature such as Google’s. Or they may entrust their password and deletion instructions to a friend or advisor. What about the decedent who leaves evidence that his or her intent was to prevent access or mandate the destruction of all content in an account, but fails to leave the login or password information? Some experts suggest that a client who wishes to maintain his or her privacy after death should use a secret account, because heirs who are unaware of it cannot request access to its contents. Jonathan J. Darrow & Gerald Ferrera, Who Owns a Decedent’s E-Mails: Inheritable Probate Assets or Property of the Network?, 10 N.Y.U. J. Legis. & Pub. Pol’y 281, 289 (2007).

The situation becomes more complicated when the content the decedent directs to be destroyed has monetary value. It would seem that situation should be treated no differently from that of a celebrity or famous author who mandates the destruction of printed files.

Protecting the Decedent’s Identity

It is now imperative to take basic precautions against identity theft, including cancelling credit and charge accounts as soon as possible, sending copies of the death certificate to the three major credit-reporting bureaus: Equifax, Experian, and TransUnion; obtaining free credit reports from each credit bureau to ensure no post-death activity; and canceling the decedent’s driver’s license at the state motor vehicle department and asking the department to refuse any requests for duplicates.

Caution in Using Commercial Services to Hold Your Digital Assets

A new cottage industry has sprung up to provide a type of “on-line safe deposit box” to store digital assets and provide a means by which designated individuals can gain access to your digital assets. A few words of caution are in order. First, be careful and make sure the testator is dealing with a reputable company. Giving someone the keys to her digital existence would be a gold mine for someone bent on stealing her identity. Second, remember that giving someone access to information about an asset is not the same as giving that asset to that individual. The testator’s will or trust should ultimately control who should inherit her assets, not an on-line service provider. Complex legal and tax issues may need to be taken into account in designating beneficiaries of virtual assets. For example, one on-line service provider refers to an “electronic will.” In most states, a will requires certain formalities—typically a written instrument signed before two witnesses—and the absence of these formalities can render one’s good intentions legally invalid.

Many on-line companies provide what is essentially an “on-line safety deposit box” for passwords and account information. Tread carefully when evaluating “digital afterlife planning sites” as such representations may lead to future litigation. Indeed, the U.S. General Services Administration has recommended that people set up a “social-media will,” which has the potential to create conflicts between legally executed wills and other new and untried efforts to create estate plans. Kelly Greene, Passing Down Digital Assets, Wall St. J. (Aug. 31, 2012).
Conclusion

As with most estate planning, the challenges and complexities are dependent on each client’s individual needs and circumstances. Navigating the best estate plan is always an adventure, but with the added layers of numerous on-line accounts and information stored by nearly everyone, an estate planner’s mission to provide excellent service must be met with considerate planning for digital assets.

Although UFADAA provides a predictable manner in which a fiduciary, consistent with well-established fiduciary law, can deal with on-line accounts and assets, the best plan for managing digital assets should be outlined in the estate plan. UFADAA will allow fiduciaries and on-line providers to comply with the current law without inadvertent exposure to federal laws and allow fiduciaries to marshal and distribute digital assets. But fiduciaries need the best information on how such digital assets are to be managed and distributed; the estate plan is the road map to assure such intentions are met.

This dynamic area of law continues to be in flux. Indeed, the Uniform Law Commission adopted a revised UFADAA at its annual meeting in July 2015. Check with http://uniformlaws.org for updates.
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

Fiduciary Access to Digital Property With RUFADAA

OSB Technology Law Update
October 14, 2016
VICTORIA BLACHLY

DIGITAL ASSETS – THE LIST CONTINUES TO GROW
$635,000 for Club Neverdie

The Numbers
> 1.23 billion active users
http://en.wikipedia.org/wiki/Facebook

> 259 million active users
http://en.wikipedia.org/wiki/LinkedIn

> 500 million tweets per day
http://www.quora.com/Twitter-1/How-many-tweets-per-day-are-there-on-Twitter

> 200 million hours of videos viewed per day
http://www.youtube.com/t/press_statistics

Digital Asset Users

- 2011 McAfee Survey: Average value of a person’s digital assets - $55,000
- Future Charitable Donations
- Average number of passwords per individual: 25
- 85% of U.S. adults use internet
- 72% of U.S. adults use social networking site
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

Preferred Banking Methods

Preferred Banking Method 2013
U.S. adults 18+

Source: American Bankers Association
http://www.aba.com/PressRoom/093010PreferredBankingMethod.htm

CHALLENGES

Upon receipt of a copy of a death certificate your Account may be terminated and all Content within your Account deleted.
TERMS OF SERVICE AGREEMENTS (“TOSA”)
HAVE YOU READ YOURS?

Yahoo: No Right of Survivorship and Non-Transferability. You agree that your Yahoo account is non-transferable and any rights to your Yahoo ID or contents within your account terminate upon your death.

Pearls Before Swine cartoon:
http://www.gocomics.com/pearlsbeforeswine/2015/12/20
In Re Justin Ellsworth

Why So Difficult?

- State Anti-Hacking Laws: ORS 164.377 Computer crime
  - (4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.
- Class A misdemeanor
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

Federal Law

Stored Communications Act ("SCA")

Contents of Digital Accounts:
SCA prohibits certain providers of public communications services from disclosing the contents of its user's communications.

Non-Content Information:
SCA allows providers to divulge non-content information, such as the user's name, address, connection records, IP address and account information, because the SCA only prohibits the disclosure of the contents of communications.

18 U.S.C. §§ 2701-2711

- 18 U.S.C. Section 2702:
  - Prohibits an electronic communication service or a remote computing service from knowingly divulging the contents of a communication that is stored by or carried or maintained on that service.
  - Unless disclosure is made “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”.

Law and Policy at the Bleeding Edge: 2016 Technology Law Updates
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

COMPUTER FRAUD & ABUSE ACT ("CFAA"), 18 U.S.C. §1030

- Prohibits unauthorized access to computers.
- The U.S. Department of Justice takes the position that this Section supports a **criminal charge** when **anyone** “exceeds authorized access” by violating the access rules set forth in the provider’s terms of service ("TOS") agreement.
- There is **NO** specific exemption or authorization in the CFAA for fiduciaries attempting to access a decedent’s digital assets.

Legislative Developments

![Oregon Map](image1)
![United States Map](image2)
Uniform Fiduciary Access to Digital Assets Act (“UFADAA”)

- Developed by ULC
- Moved forward quickly
- Hard fought by some online providers
- ACLU concerned about privacy issues

Privacy Expectation Afterlife and Choices Act (“PEAC”)

- Social Media Bill
- Requires Court Order (Probate)
  - Avoiding Probate will no longer be an option
  - Court Finding: Disclosure will not violate the Stored Communications Act and other federal law
- Estate required to indemnify service provider from liability
- PRs and administrators must provide extensive documentation to get order
- Service provider can object to order if unduly burdensome
- Terms of Service Agreement still controls
REVISED UFADAA

- Brings fiduciary law into the internet age
- Gives Account Holders Some Control over their Digital Assets
- Authorizes the following fiduciaries:
  - Executors and personal representatives
  - Guardians and conservators
  - Trustees
  - Agents under power of attorney

RUFADAA

**Section 3 – Applicability**

- Governs actions of fiduciary or agent acting under a will, trust or POA executed before, on or after effective date.
- Conservatorships.
- Applies to Custodians of digital assets or users who reside in a state or resided there at death.
- Inapplicable to digital assets of employers’ digital assets used by employees in ordinary course of employer’s business.
Chapter 1—War and PEAC: Negotiating with the Tech Industry over Fiduciary Access to Digital Property

RUFADAA

Section 4 - Hierarchy
- Visible on-line tool directions.
  - FB Legacy Contacts
  - Google Inactive Account Manager
- Will, trust, POA or other records.
- TOSAs govern access for those who pass without a plan.

Section 6 – Custodial Options for Disclosing
- Grant full access to fiduciary (unlikely to be popular);
- Grant partial access to account sufficient to perform tasks necessary to discharge duties; or
- Data dump.
  May charge reasonable fee and need not disclose assets deleted by user.
Section 6 – Custodial Procedures for Disclosing

- If custodian considers request unduly burdensome, fiduciary or custodian may ask court for order to:
  - Disclose a subset;
  - Disclose all or none;
  - Disclose to court for in camera review.

Sections 7 & 8 – Disclosure to Personal Representative

Each section has protected (letter) and non-protected (envelope) sections.

If user consented to disclosure, PR provides:

- Written request;
- Death certificate;
- Certified copy of letter of appointment; &
- Copy of user’s consent, if not through online tool.

If Custodian requests, must also provide number, username, or address of account, evidence linking user to account or court order finding that user had specific account, disclosure would not violate federal law, user consented or that disclosure is reasonably necessary for estate administration.
Sections 9 & 10 – Disclosure to Agent
If user consented to disclosure, PR provides:

- Written request;
- POA (“hot power”) or other record;
- Certification that power is in effect; &
- If requested, information linking account to principal.

Sections 11, 12 & 13 – Disclosure to Trustee
If Trustee is initial user, then consent presumed.
If Trust grants access:
- Written request;
- Trust certification; &
- If requested, information linking account to Trust.
**Section 14 – Disclosure to Conservator/Guardian**

Conservator may have access after opportunity for a hearing, unless protected person or court otherwise directs.

Envelope only – online providers don’t want living people with accounts where impersonation occurs.

Make ask custodian to suspend or terminate for good cause.

**Fiduciary Duty & Authority**

**Section 15**

- Delineates fiduciary duties and limits on fiduciary authority.
- Subject to TOSA, copyright & other law.
- Authority not held in accounts.
- Cannot impersonate user.
- Authorized user.
- Can request termination of account.
- Access anywhere.
Section 16 – Compliance & Immunity

Custodian must comply within 60 days. 
Mandates what SCA permits. 
Immunity for custodian compliance.

NEED FOR REFORM

Without RUFADAA, fiduciaries are (arguably) violating state and federal law every time they access online accounts and information, EVEN IF the decedent had the wherewithal to write down their password in advance.
Digital Asset Planning

Dialogue with client

1. Why?
   - Prevent financial loss to estate
   - Avoid loss of photos, memories, or story
   - Protect secrets
   - Avoid identity theft
   - Assist families and fiduciaries

UPDATE FORMS & EDUCATE

- Add comprehensive language to POA, Trust, and Will authorizing access.
- Digital Asset Authorization form.
- Danger of “digital will.”
- Use of online lockboxes.
- VAIL or Digital Asset Inventory Form. (see Jim Lamm’s at [www.digitalpassing.com/digital-audit](http://www.digitalpassing.com/digital-audit))
Virtual Asset Instruction Letter

**IDENTIFY ACCOUNTS:**

**INSTRUCTIONS: MAINTAIN**

**INSTRUCTIONS: DELETE**

**MAINTAIN: LIST OF ACCOUNTS**

**SELECT PEOPLE TO HANDLE ASSETS:**

**UPDATE WILL & TRUST**

**UPDATE POWER OF ATTORNEY**

“Don’t believe everything you read on the Internet just because there’s a picture with a quote next to it.”

—Abraham Lincoln
Technology and Agriculture: Emerging Trends and Legal Issues

JENNY DRESLER
DIRECTOR OF STATE PUBLIC POLICY
OREGON FARM BUREAU FEDERATION

MARY ANNE NASH
PUBLIC POLICY COUNSEL
OREGON FARM BUREAU FEDERATION

Agriculture Technology Legal Issues

BIOTECHNOLOGY
CROP DEVELOPMENT
DRONES
FARM DATA
### Biotechnology

**FEDERAL REGULATION**  
**STATE AND LOCAL BALLOT MEASURES**  
**STATE LEGISLATIVE ACTIONS**  
**FEDERAL ACTION**

---

**Plants**

- **Selective Breeding** ("traditional breeding") looks for and cross-breed plants that had the characteristics they wanted.
- **Mutagenesis** ("mutation breeding") changes DNA by exposing seeds to chemicals or gamma irradiation and then selecting the plants with the desired traits.  
  - 3,200+ varieties, including red grapefruit, bananas, peanuts, peppermint and organic rice
- **Genetic Engineering** ("GMO") selects a trait that exists in nature and inserts the gene into the target plant. Breeders can make changes in a plant’s makeup without any insertions, for example, by silencing ("turning off") existing genes.

**Animals**

- A **transgenic** animal carries a known sequence of recombinant DNA in its cells, and which passes that DNA onto its offspring.  
  - Recombinant DNA means DNA fragments that have been joined together in a laboratory, designed to express the proteins that are encoded by the genes.  
  - Examples include:
    - Therapeutic proteins for the treatment of human diseases
    - Proteins that enable animals to better resist disease
    - Proteins that produce more healthful animal products for consumers.
- **AquAdvantage®** Salmon was approved for sale in the U.S in 2015

---

Definitions

<table>
<thead>
<tr>
<th>Plants</th>
<th>Animals</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Selective Breeding (“traditional breeding”) looks for and cross-breed plants that had the characteristics they wanted.</td>
<td>• A <strong>transgenic</strong> animal carries a known sequence of recombinant DNA in its cells, and which passes that DNA onto its offspring.</td>
</tr>
</tbody>
</table>
| • Mutagenesis (“mutation breeding”) changes DNA by exposing seeds to chemicals or gamma irradiation and then selecting the plants with the desired traits.  
  - 3,200+ varieties, including red grapefruit, bananas, peanuts, peppermint and organic rice | Recombinant DNA means DNA fragments that have been joined together in a laboratory, designed to express the proteins that are encoded by the genes.  
Examples include:
  - Therapeutic proteins for the treatment of human diseases
  - Proteins that enable animals to better resist disease
  - Proteins that produce more healthful animal products for consumers. |
| • Genetic Engineering (“GMO”) selects a trait that exists in nature and inserts the gene into the target plant. Breeders can make changes in a plant’s makeup without any insertions, for example, by silencing ("turning off") existing genes. | |
**Why Farmers Grow GE Crops**

- As of 2014, GE plants are grown globally on over 181 million hectares by 18 million farmers in 28 countries.
- GE varieties provide several benefits to farmers, such as through reduced chemical pesticide use, increased crop yields, reduced water and resource use, preservation of soil, and increased farmer profits.
- In the U.S., farmers have planted GE varieties of corn, soy beans, cotton, canola, sugar beets, alfalfa, papaya, and squash.

---

**Regulation of GE Crops**

- The United States Food and Drug Administration, the Food and Drug Administration, and the Environmental Protection Agency all regulate GE crops.
- Prior to the commercialization of GE crops, all three agencies will have determined that the GE crop is deemed “substantially equivalent” to its conventional variety for federal regulatory purposes.
- Once GE crops are deregulated, they can be planted anywhere in the United States.
Legal Agreements – GE Crops

- Biotechnology companies and seed distributors that market GE seeds to farmers usually require that farmers sign grower agreements.
- These agreements generally give the farmer rights to plant GE seeds and harvest the crop that's grown, but do not allow the farmer to save and replant seeds from the crop.
- The agreements often have provisions governing where and how the GE seed will be planted.

Legal Agreements – Key Provisions
(Monsanto Contract)

- Read and follow the Technology Use Guide and Insect Resistance Management/Grower Guide.
- Only buy seed from a dealer or seed company licensed by Monsanto.
- Use seed with Monsanto patented technology solely for planting a single commercial crop.
- Agreed to only export and plant these crops in countries that allow them.
Oregon Seed Preemption

- **SB 863 (2013 Special Session)**
  Prevents local governments from regulating agricultural seed and nursery stock, including biotech crops
  - Not about *whether* agricultural seed is regulated, but rather *where* that regulation takes place.
  - Prevents a patchwork of regulations across county lines
  - Exemption for initiative in Jackson County

Coexistence: Mediation Bill (2015)

- Product of work group on GMOs. Statewide policy to incentivizes grower-to-grower communication and facilitate conflict resolution without legislative intervention.
- If a farmer believes they are being impacted by another farmer's operation, they can request mediation by ODA or USDA.
- If the neighbor is not willing to go to mediation, that can become a factor for a court in determining whether to grant injunctive relief.
- Makes mediation mandatory for grower to grower lawsuits unless both parties waive mediation.
Biotechnology on the Ballot: County Initiatives

- **Jackson County Genetically Modified Organism Ban**, Measure 15-119 (May 2014)
  Passed on a 3:2 margin
- **Josephine County Genetically Modified Organism Ban**, Measure 17-58 (May 2014)
  Preempted by SB 863
- **Benton County "Local Food System Ordinance" Genetically Modified Organism Ban**, Measure 2-89 (May 2015)
  Failed on nearly 3:1 margin

Biotechnology on the Ballot: Measure 92

- **State GMO labeling**
  State-specific mandate
  Increased red tape on farmers, food companies, and grocery stores
  Would require farmers and food producers to separate, re-package and re-label their products *just for Oregon*
- **Failed on the November 2014 Ballot**
  NO: 50.03%
  YES: 49.97%
National GMO Labeling: S. 764

- Vermont Act 120 (2014) required labels on products containing genetically engineered ingredients
- “National Bioengineered Food Disclosure Standard” (July 2016)
  - Directs the U.S. Department of Agriculture (USDA) to “establish a national mandatory bioengineered food disclosure standard”
  - Consistent, uniform labeling standard
  - Allows use of QR codes or 1-800 numbers as a form of GMO labeling
  - Preempts the State of Vermont’s law and other state labeling laws

CRISPR-Cas9 Technology

- Precise gene-editing technique that researchers to remove and replace bits of DNA in a much more targeted way than previous genetic modification techniques
- Does not contain any introduced gene material or foreign DNA
- Is not regulated by USDA at present, due to fact that it does not present a threat to other plants
- Monsanto has licensed the use of CRISPR-Casgenome-editing technology to increase:
  - Plant productivity
  - Pest and disease resistance
  - Drought resistance
Other Crop Development Technology

UNIVERSITY LICENSE AGREEMENTS

Rutgers University License Programs

- Universities have also been involved in developing and licensing new varieties of agricultural crops.
- For example, Rutgers University initiated a cranberry program in 1985 to improve yield, fruit quality, and genetic diversity.
- The results of these breeding efforts has been the commercial release of five varieties of Rutgers cranberries.
Rutgers University License Agreements

- The Rutgers patented cranberry varieties are available to commercial growers in the US and Canada under license from Rutgers University.
- Growers must purchase certified vines for conventional planting from one of two grower-nurseries, which follow strict breeding and propagation guidelines.
- Rutgers retains ownership of the vines, while the growers have ownership of the fruit produced.

Other Rutgers Propagation Programs

- Rutgers has similar programs for asparagus, dogwoods, fruit trees, hazelnuts, holly, strawberries, tomatoes, and turf grass.
- Other universities around the United States have similar programs, which are often heavily invested in by the state and federal governments to ensure the high yield, quality crops.
Drone Regulation In Oregon

OREGON LEGISLATION

FEDERAL LEGISLATION

HB 2710 (2013)

- Most comprehensive in U.S.
- Very tight restrictions on use of images or information obtained by UAS
  - Privacy protections (treble damages)
  - Due Process/Warrantless Search protections
  - No weaponization allowed by public bodies
  - Preemption of local regulation
  - Protection of legal uses
Drones: 2015 and 2016

- **HB 2354 (2015)**
  Removed 400 foot restriction (pre-empted by federal law) and replaced the term “drone” with “unmanned aircraft system”

- **HB 4066 (2016)**
  Prohibits weaponizing UAS by all users
  Clarifies FAA approved operations still subject to civil actions (privacy/nuisance/trespass/etc.)
  Creates violation of interfering with other aircraft
  Requires public bodies to develop policies to protect information gathered by UAS
  Allows flights over private property with FAA authorization
  Prohibits flights near critical infrastructure with landowner exceptions

FAA Regulations

- **FAA Small UAS rules (under 55 pounds with payload)** effective August 29, 2016 requires UAS operators to:
  - Fly below 400 feet
  - Fly within visual line-of-sight
  - Do not fly over groups of people
  - Do not fly over stadiums and sporting events
  - Do not fly within 5 miles of an airport
  - Do not fly near emergency operations
  - Do not fly near other aircraft
  - Do not fly under the influence
Farm Data

HOW IS FARM DATA PROTECTED?

Farm Data: The next legal frontier?

- Farmers today utilize the latest technology to collect data about almost every facet of their cropping operations from planting through harvest.
- Farmers have growing concerns about who owns this data, and how to balance the advantages of its collection by third parties (such as equipment dealers, input vendors, and consultants) with the potential loss of confidentiality in such transfers.
Farm Data

- A recent Drake law review article suggests that the current intellectual property framework fails to provide a clear niche for farm data in the realms of trademark, patent, or copyright law.
- They concluded that to whatever extent farm data comprises legally-protectable intellectual property owned by the farmer, producers wanting to maximize their claim of rights in farm data should carefully manage their data disclosures through clear agreements with those with data access.

Questions?

Jenny Dresler
Jenny@oregonfb.org

Mary Anne Nash
Maryanne@oregonfb.org

Thank you!
Chapter 3

Drone Law: Updates and Guidance—Presentation Slides

CRAIG RUSSILLO
Schwabe Williamson & Wyatt
Portland, Oregon
Drone Law: Updates and Guidance

A primer on the permitted uses of drones under federal and state law, privacy concerns and liability and insurance issues.

TOPICS COVERED

- Federal law governing operation of drones
  - Recreational and commercial use
- Preemption
  - Interplay between state and federal law
- Liability and insurance concerns.
JARGON ˈJÄrgəN/ NOUN  
SPECIAL WORDS OR EXPRESSIONS THAT ARE USED BY A PARTICULAR PROFESSION OR GROUP AND ARE DIFFICULT FOR OTHERS TO UNDERSTAND.

• UAS: Unmanned Aircraft System  
  – unmanned aircraft and associated elements (including communications links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.

• UAV: Unmanned Aerial Vehicle  
  – aircraft with no pilot on board that can be remote controlled or can fly autonomously based on preprogrammed flight plans or more complex dynamic automation systems.

JARGON ˈJÄrgəN/ NOUN  
SPECIAL WORDS OR EXPRESSIONS THAT ARE USED BY A PARTICULAR PROFESSION OR GROUP AND ARE DIFFICULT FOR OTHERS TO UNDERSTAND.

• UA: Small Unmanned Aircraft System  
  – Weighing less than 55 lbs. with everything attached  
  – Can be flown w/o possibility of direct human intervention from within or on the aircraft

• BVLOS: Beyond Visual Line of Sight  
  – Prohibited under current FAA regulations

• NAS: National Airspace System  
  – According to FAA, everything above the ground

• VO: Visual Observer

• PIC: Pilot In Command
WHAT IS A DRONE?

GENERAL ATOMIC MQ-9 REAPER

• Used by USAF and CIA
• Over past 5 years estimated 2,400 deaths from drones.
HUBSAN X4 MINI H107C+ QUADCOPTER WITH 720P CAMERA

Dimensions 4.2 x 4.2 x 1.4" / 106.7 x 106.7 x 35.6 mm
Weight 1.9 oz / 53.9 g

MOST COMMON DRONES

DJI Phantom

3D Robotics Solo
WHO CAN FLY DRONES?

- Recreation/Hobby
- Commercial

WHAT LAWS GOVERN THE USE OF DRONES?

- Federal
- State
SECTION 336 OF FAA MODERNIZATION AND REAUTHORIZATION ACT OF 2012, 49 USC 4010 (FMRA) PROHIBITS REGULATION OF "MODEL AIRCRAFTS" (I.E., HOBBYISTS)

(a) In General.—Notwithstanding any other provision of law relating to the incorporation of unmanned aircraft systems into Federal Aviation Administration plans and policies, including this subtitle, the Administrator of the Federal Aviation Administration may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft, if—

(1) the aircraft is flown strictly for hobby or recreational use;

(2) the aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;

(3) the aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;

(4) the aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and

(5) when flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation (model aircraft operators flying from a permanent location within 5 miles of an airport should establish a mutually-agreed-upon operating procedure with the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport)).

FEDERAL LAW GOVERNING HOBBYISTS / RECREATIONALIST FAA ADVISORY CIRCULAR AC 91-57 (1981)
Chapter 3—Drone Law: Updates and Guidance—Presentation Slides

WHAT IS HOBBY OR RECREATIONAL USE?

Hobby or recreation
- Flying a model aircraft at the local model aircraft club.
- Taking photographs with a model aircraft for personal use.
- Using a model aircraft to move a box from point to point without any kind of compensation
- Viewing a field to determine whether crops need water when they are grown for personal enjoyment.

Not hobby or recreation
- Receiving money for demonstrating aerobatics with a model aircraft.
- A realtor using a model aircraft to photograph a property that he is trying to sell and using the photos in the property’s real estate listing.
- A person photographing a property or event and selling the photos to someone else.
- Delivering packages to people for a fee (“free shipping” prohibited).
- Determining whether crops need to be watered that are grown as part of commercial farming operation.

REGISTERING YOUR DRONE

- Does not apply to commercial use of drones
- Must weigh over .55 lbs. but less than 55 lbs.
- 13 years of age or older (if the owner is less than 13 years of age, a person 13 years of age or older must register the small unmanned aircraft)
- A U.S. citizen or legal permanent resident
- $5 cost for three years

OWN A DRONE? REGISTER YOUR DRONE

registermyuas.faa.gov
FEDERAL LAW AND COMMERCIAL USE OF DRONES

FAA Modernization and Reform Act of 2012

14 CFR Part 107 - i.e., “Small UAS Rule”
- Effective August 29, 2016

FAA Reauthorization Act of 2016

BEFORE PART 107

- FAA's position: commercial use of drones prohibited under federal law
- Section 333 of FMRA allowed Sec. of Transportation to provide “exemptions” from federal regulations
- Case-by-case review; time-consuming & $$$
  - Pilot's license
  - No BVLOS
  - Visual observer
PART 107 HIGHLIGHTS

- Limits on operation
- Remote Pilot In Command Certificate vs. Pilot's License
- Waiver process.

DRONE OPERATIONS

- 100 mph
- 400 feet AGL (above ground level); exception if within 400 feet of structure
- Cannot operate over people not participating in UAS operations unless "covered"
- No BVLOS
- Autonomous operations allowed (sort of)
- Visual observer no longer needed
- Need ATC permission before operating in Class B, C, D, or E airspace
DRONE OPERATIONS

- No careless or reckless operations
- One sUAS at a time
- Remote PIC need not be controlling drone
- Transportation of property (i.e., delivery) allowed, but
  - Must be within bounds of state
  - Must be within VLOS
  - Cannot be used from a moving vehicle
- Daylight operations / civil twilight
- Use from moving vehicle only over sparsely-populated area

REMOTE PILOT CERTIFICATION

- Replaces pilot-license requirement under 333
- Eligibility
  - 16 years of age
  - Able to read, speak, write, and understand English
  - Physically and mentally able to operate sUAS
  - Pass initial aeronautical knowledge test
  - TSA vetting
CERTIFICATE OF WAIVER

Part 107 allows FAA Administrator to waive certain provisions:
1. Operating from moving vehicle (not for deliveries)
2. Daylight operations
3. BVLOS
4. Operation of multiple sUAS
5. Yielding the right of way
6. Operations over people
7. Operations in certain airspace
8. Operating limitations for small sUAS.

Online application process.
96 granted

2016 FAA REAUTHORIZATION ACT

- Extended FAA Authorization until 2017
- Made federal crime to interfere with wildfire suppression efforts.
- $20,000 fine
STATE VS. FEDERAL
CONFLICT AND PREEMPTION

ORS 837.380

Allows property owners to sue a drone operator if

(1) a drone has flown less than 400 feet above the owner’s property at least once,

(2) the property owner has told the drone operator that he/she does not consent to the drone flying over his/her property, and

(3) the operator then flies the drone less than 400 feet above the property again.

If these three conditions are met, the property owner can seek injunctive relief, “treble damages for any injury to the person or the property,” and attorney fees if the amount of damages is under $10,000.
PREEMPTION IS OPEN ISSUE

• Part 107 does not include preemption provision.
• FAA position:
  “The FAA is not persuaded that including a preemption provision in
  the final rule is warranted at this time. Preemption issues involving
  small UAS necessitate a case-by-case specific analysis that is not
  appropriate in a rule of general applicability…certain legal aspects
  concerning small UAS use may best be addressed at the State or
  local level. For example, State law and other legal protections for
  individual privacy may provide recourse for a purpose whose
  privacy may be affected through another person’s use of a UAS.”

FAA “STATE AND LOCAL REGULATION OF
UNMANNED AIRCRAFT SYSTEMS FACT SHEET.”
DECEMBER 17, 2015

State and local laws that would require FAA consent
• Operational restrictions on flight altitude, flight paths; operational
  bans; any regulation of the navigable air space.
• Mandating equipment or training for UAS related to aviation safety
  such as geo-fencing.

State and local laws not requiring FAA consent
• Requirement for police to obtain a warrant prior to using a UAS for
  surveillance.
• Specifying that UAS may not be used for voyeurism.
• Prohibitions on using UAS for hunting or fishing, or to interfere
  with or harass an individual who is hunting or fishing
• Prohibitions on attaching firearms or similar weapons to UAS.
CAN YOU SHOOT DOWN A DRONE?
**BOGGS V. MEREDITH (AKA THE “DRONE SLAYER”)**

- William Meredith shot down hovering drone (200 feet above property)
- Acquitted of state criminal charges
- Drone (Boggs) owner sued: USDC W D. Ky. 3:16-cv-6, alleged:
  - (1) Dec. Judgment
    - Drone is aircraft
    - Flying in class G “navigable airspace”
    - Exclusive jurisdiction of US not Boggs’ property / did not violate expectation of privacy
  - (2) Trespass to chattels ($1,500 claim)
  - 1st federal case of drone operator v. property owner

PRIVACY AND DRONES

“[T]he Department of Commerce, through the National Telecommunications and Information Administration…will initiate this multi-stakeholder engagement process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS use."
- President Obama
  July 15, 2015.
NTIA VOLUNTARY BEST PRACTICES
JUNE, 2016

• Inform others of your use of UAS
• Show care when operating UAS or collecting and storing covered data
  – “Covered data” means information collected by a UAS that identifies a particular person.
• Limit the use and sharing of Covered Data
• Secure Covered Data
• Monitor and comply with evolving federal, state, and local UAS laws.

ORS 837.380

Allows property owners to sue a drone operator if

(1) a drone has flown less than 400 feet above the owner’s property at least once,

(2) the property owner has told the drone operator that he/she does not consent to the drone flying over his/her property, and

(3) the operator then flies the drone less than 400 feet above the property again.

If these three conditions are met, the property owner can seek injunctive relief, “treble damages for any injury to the person or the property,” and attorney fees if the amount of damages is under $10,000.
LIABILITY AND INSURANCE ISSUES

- 1st and 3rd Party claims
- No insurance requirements in Part 107
- Standard GL policy may not cover drone operations
- Best practice: traditional aviation insurer

DRONE INSURANCE RISKS

- First Party: Coverage for loss of property
  - Hull coverage
  - Cameras / add-ons
  - Named perils or all risk
  - Valuation provision

- Third Party: coverage for liability
  - Property / life
  - Privacy & Data Breach
  - Trespass, negligence
Since 1997, Craig Russillo has been helping clients resolve complex commercial disputes, particularly with respect to borrowing, lending and real estate. Craig works extensively with lenders and creditors in judicial and non-judicial foreclosures, representing their interests in state, federal and bankruptcy courts. He also has significant experience with real property disputes, including complex title issues, landlord/tenant disputes and construction matters. Craig is the firm’s point-person with respect to the burgeoning area of drones.
Oregon Energy & Climate Policy

KRISTIN EBERHARD, SIGHTLINE INSTITUTE

OCTOBER 14, 2016
May 2016  L-OTI (°C) Anomaly vs 1951-1980  0.95

Days above 100°F

1990-2010

Phoenix 92 days

Dallas 15
Acidifying ocean hurts shellfish industry

Worsens asthma and respiratory health
Reduces snowpacks

Exacerbates wildfires
Should Oregon have stronger regulations to:

- Invest in Public Transit
- Carbon Tax
- Polluters Pay
- Reduce GHG emissions

Data shows:

- Strongly Yes
- Somewhat Yes
- Neutral/Don’t know
- Somewhat No
- Strongly No

Oregon aims to reduce greenhouse gas emissions

“it is the policy of this state to reduce greenhouse gas emissions”:

- Stop rising by 2010
- 10% below 1990 levels by 2020
- 75% below 1990 levels by 2050

- Bill passed in 2007
Formula for reducing emissions

Population \times \frac{Services}{Person} \times \frac{Energy}{Service} \times \frac{Emissions}{Energy} = \text{Emissions}
Oregon’s population is growing

Source: Oregon Department of Economic Analysis

Oregon's emissions per capita are less than the US average but higher than other states and countries.

Source: Oregon Department of Economic Analysis
Oregon GHG Emissions

Biggest sources are transportation and electricity emissions.

Oregon’s greenhouse gas pollution comes mainly from transportation, electricity, and natural gas emissions.

Total 2012 emissions = 60 MMT

- Electricity 30%
- Transportation 39%
- Natural Gas 10%
- Agriculture 9%
- Other 6%
- Industrial 6%

Source: Oregon Department of Environmental Quality
Electricity sector opportunities

Population x Cool Air kWh x Emissions
Person x Cool Air kWh = Emissions

Switch to cleaner resources

Population x Cool Air kWh x Emissions
Person x Cool Air kWh = Emissions
Renewable Portfolio Standard

Oregon: 50% by 2040
- Bill passed in 2016
- Solar, wind, hydropower, ocean power, geothermal, municipal solid waste, and biomass, including biogas.
- Applies to large investor-owned utilities
- Consumer-owned utilities: 25% by 2025
- Small utilities: 10% by 2025

California: 50% by 2030
- Bill passed in 2015

Washington: 15% by 2020
- Ballot initiative in 2006

Use more efficient devices

\[
\text{Population} \times \frac{\text{Cool Air} \text{ kWh}}{\text{Person}} \times \frac{\text{Emissions}}{\text{Cool Air kWh}} = \text{Emissions}
\]
Energy Efficiency (technological)

- Appliance standards
- Building codes
- Utility Programs

Use less

\[
\text{Population} \times \frac{\text{Cool Air}}{\text{Person}} \times \frac{\text{kWh}}{\text{Cool Air}} \times \frac{\text{Emissions}}{\text{kWh}} = \text{Emissions}
\]
Conservation (behavioral)

- Smaller house or office space
- Raising the thermostat

Conservation (policies)

Make “missing middle” housing legal
Transportation

Transportation sector opportunities

\[
\text{Population} \times \frac{\text{Miles}}{\text{Person}} \times \frac{\text{Gallon/kWh}}{\text{Mile}} \times \frac{\text{Emissions}}{\text{Gallon/kWh}} = \text{Emissions}
\]
Switch to cleaner fuels

Population \times \frac{\text{Miles}}{\text{Person}} \times \frac{\text{Gallon/kWh}}{\text{Mile}} \times \frac{\text{Emissions}}{\text{Gallon/kWh}} = \text{Emissions}

Clean Fuels Standard

Reduce carbon content of fuels 10% in 10 years. Switch to biofuels and electricity.

- Bill passed 2015
Use more efficient vehicles

Population \times \frac{\text{Miles}}{\text{Person}} \times \frac{\text{Gallon/kWh}}{\text{Mile}} = \frac{\text{Emissions}}{\text{Gallon/kWh}}

Vehicle Standards
Federal fuel efficiency (CAFÉ) standards
- Improve miles per gallon

State Clean Cars Rule
- Improve GHG per mile
- Adopted rules in 2006 and updated in 2013
Right-sized vehicles

Right-sized vehicles
Right-sized vehicles
Right-sized vehicles
Right-sized vehicles

Travel less

Population \times \frac{\text{Miles}}{\text{Person}} \times \frac{\text{Gallon/kWh}}{\text{Mile}} \times \frac{\text{Emissions}}{\text{Gallon/kWh}} = \text{Emissions}
Land Use Planning

Urban growth boundary

20-minute neighborhoods

Pollution Pricing

(CAP OR TAX PER TON)
Countries and states already charge to pollute

Carbon Pricing Around the World

North American Climate Pollution Pricing Programs

- Green bubble sizes indicate amount of climate pollution regulated by price.
- Orange bubbles indicate amount of pollution that could potentially be regulated by price.
How does price interact with other policies?

Analyzing by cost
Analyzing by wedge

Pollution price plus other policies

Source: Oregon Global Warming Commission
Important policy questions:

1. Does it apply to most pollution?
2. Does the price ramp up?
3. What do we do with the money?
Good answers:

1. Does it apply to most pollution?
   - Yes ~ 85%

2. Does the price ramp up?
   - Yes – to over $100/ton my mid-century

3. What do we do with the money?
   - Mitigate price impacts; invest

Lower income households spend more of their income on energy.

Percentage of Household Income Spent on Energy by Income Quintile

Source: Consumer Expenditure Survey, 2011
A flat rebate can make lower-income households better off.

Percentage change in after-tax household income with a carbon price plus rebate, by quintile

Source: Congressional Budget Office, 2007

How has pricing worked elsewhere?
BC reduced transportation fuel use 15% in 4 years.

Sales of refined petroleum products per capita (2007 = 100%)

Source: CANSIM 134-0004, 051-0001

BC’s economy is fine.

Real GDP per capita (2007=100%)

Source: CANSIM 384-0038, 051-0001
RGGI invested in energy efficiency and created jobs

- Energy Efficiency, 58%
- Bill Assistance, 15%
- General Fund, 12%
- Clean Energy, 5%
- Administration, 5%
- Other Emissions Reductions, 5%

Clean energy creates more jobs than fossil fuels

- Direct jobs created per $1 million spent
- Indirect jobs created
- Induced jobs created

- Building Retrofits
- Solar
- Smart Grid
- Coal
- Oil and Natural Gas
RGGI’s economy is fine.

Northeast States compared to the rest of the US

California invests in disadvantaged communities

- Transit, $19
- Weatherization of Homes, $75
- Urban Forestry, $18
- Affordable Housing (near Transit), $65
- Electric Vehicles (passenger and freight), $115
California is on track to meet its 2020 goal

Source: Lawrence Berkeley National Labs, 2013

California’s economy is fine.

Source: Next10, California Green Innovation Index, 2014
CA is growing clean energy jobs.

Source: Next10, California Green Innovation Index, 2014

Possible answers in Oregon:

1. 85% (transportation, electricity, natural gas and large industrial)
2. Ramps to $100 per ton or more by mid-century
3. Ensure prosperity, equity and viability
Oregon not on track to meet statutory goals

Oregon faces legal limitations on use of money
What the pollution revenue pie might look like in Oregon

Highway Fund Subaccount, $439
Electricity & NG Bill Assistance, $315
Oregon Climate Investment Fund, $114
Just Transition, $19
EITE Industries, $57

Reserve, $10

~$1 Billion in 2020

What’s next?
2017 Oregon Legislative Session

Transportation package
- Better transit and land use planning?
- More local control?
- A carbon adder?

Cap and trade bill?

Formula for reducing emissions

Population x Services x Energy x Emissions = Emissions

Population

Services

Energy

Emissions

Person

Service

Energy

Emissions
Thank you.

KRISTIN@SIGHTLINE.ORG
Oregon GHG emissions by source

Figure 1: Oregon Emissions by Sector, 1990-2012 (Million Metric Tons of Carbon Dioxide Equivalent)

Source: Oregon Global Warming Commission
Stingray Technology & Associated Legal Issues

Oregon State Bar
Continuing Legal Education (CLE)

Stingray
FOURTH AMENDMENT
U.S. CONSTITUTION

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
Katz v. United States
389 U.S. 347, 353 (1967)

The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

Id. at 361
(Harlan, J. concurring)

[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as “reasonable.”
[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as “reasonable.” Thus a man’s home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the “plain view” of outsiders are not “protected” because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

*California v. Ciraolo,*
(internal citations omitted)

The observations by [the police] in this case took place within public navigable airspace, in a physically nonintrusive manner; from this point they were able to observe plants readily discernible to the naked eye as marijuana. . . . Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. On this record, . . . respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor.
United States v. Miller,

[C]hecks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

California v. Greenwood,
(internal quotations & citations omitted)

[R]espondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection. It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so. Accordingly, having deposited their garbage in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it, respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded.
**Smith v. Maryland,**
442 U.S. 735, 741-43 (1979)

In applying the *Katz* analysis to this case, it is important to begin by specifying precisely the nature of the state activity that is challenged. The activity here took the form of installing and using a pen register. Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his "property" was invaded or that police intruded into a "constitutionally protected area." Petitioner's claim, rather, is that, notwithstanding the absence of a trespass, the State, as did the Government in *Katz,* infringed a "legitimate expectation of privacy" that petitioner held. Yet a pen register differs significantly from the listening device employed in *Katz,* for pen registers do not acquire the contents of communications.

* * *

Given a pen register's limited capabilities, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.

This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. . . . Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

* * *

Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.

---

**United States v. Knotts,**
460 U.S. 276 (1983)

A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the source] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

* * *

Visual surveillance from public places along [the source]'s route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of [the source]'s automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.
United States v. Jones,
132 S.Ct. 945, 949 (2012)

The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a “search” within the meaning of the Fourth Amendment . . . .

Id. at 954-57
(Sotomayor, J., concurring)

I join the Court’s opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, “[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area.”

* * *

Nonetheless, . . . physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion’s trespassory test may provide little guidance.

* * *

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: “limited police resources and community hostility.”

* * *

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.

* * *

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., Smith, Miller. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.
Chimel v. California, 395 U.S. 752, 762-63 (1969)

When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. . . . In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. And the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule. . . . There is ample justification, therefore, for a search of the arrestee's person and the area “within his immediate control”—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.

Riley v. California 134 S. Ct. 2473 (2014)

The United States asserts that a search of all data stored on a cell phone is “materially indistinguishable” from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom. Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.

[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.
United States v. Davis,
785 F.3d 498 (11th Cir. 2015)

- six robberies at a Little Caesar's restaurant, an Amerika Gas Station, a Walgreens drug store, an Advance Auto Parts store, a Universal Beauty Salon, and a Wendy's restaurant
- the Government subpoenaed Davis’s telephone communications records around the time of the robberies from MetroPCS (without a search warrant issued on probable cause)
- records showed the telephone numbers for each of Davis's calls and the number of the cell tower that connected each call
- calls to and from Davis's cell phone were connected through cell tower locations that were near the robbery locations

Id. at 511-12
(internal quotations & citations omitted)

Like the bank customer in Miller and the phone customer in Smith, Davis can assert neither ownership nor possession of the third-party’s business records he sought to suppress. Instead, those cell tower records were created by MetroPCS, stored on its own premises, and subject to its control. Cell tower location records do not contain private communications of the subscriber. This type of non-content evidence, lawfully created by a third-party telephone company for legitimate business purposes, does not belong to Davis, even if it concerns him.

More importantly, like the bank customer in Miller and the phone customer in Smith, Davis has no subjective or objective reasonable expectation of privacy in MetroPCS’s business records showing the cell tower locations that wirelessly connected his calls at or near the time of six of the seven robberies.

Admittedly, the landscape of technology has changed in the years since these binding decisions in Miller and Smith were issued. But their holdings did not turn on assumptions about the absence of technological change. To the contrary, the dispute in Smith, for example, arose in large degree due to the technological advance from call connections by telephone operators to electronic switching, which enabled the electronic data collection of telephone numbers dialed from within a home. The advent of mobile phones introduced calls wirelessly connected through identified cell towers. This cell tower method of call connecting does not require “a different constitutional result” just “because the telephone company has decided to automate” wirelessly and to collect the location of the company’s own cell tower that connected the calls. . . . The longstanding third-party doctrine plainly controls the disposition of this case.

The use of cell phones is ubiquitous now and some citizens may want to stop telephone companies from compiling cell tower location data or from producing it to the government. . . . The recourse for these desires is in the market or the political process; in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections.
United States v. Graham,
796 F.3d 332 (4th Cir. 2015)

• six armed robberies of several business establishments located in Baltimore
• government sought cell phone information from Sprint/Nextel, the service provider for the two phones recovered from Graham’s truck, including CSLI for calls and text messages transmitted to and from both phones around the time of the robberies
• privacy policy in effect at the time Sprint/Nextel disclosed CSLI to the government stated: “Information we collect when we provide you with Services includes when your wireless device is turned on, how your device is functioning, device signal strength, where it is located, what device you are using, what you have purchased with your device, how you are using it, and what sites you visit.”

Id. at 344-45, 348, 354-55

[T]he government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user’s historical CSLI for an extended period of time. Examination of a person’s historical CSLI can enable the government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information.

* * *

Miller and Smith do not categorically exclude third-party records from Fourth Amendment protection. They simply hold that a person can claim no legitimate expectation of privacy in information she voluntarily conveys to a third party. It is that voluntary conveyance—not the mere fact that the information winds up in the third party’s records—that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone user does not “convey” CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement.

* * *

We cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person.
United States v. Karo,

[We] reject the government's contention that it would be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime ... will be committed!.] If agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, the government argues, for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises. The argument that a warrant requirement would oblige the government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.

Harris Corporation
NDA

[T]o ensure that [ ] wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including but not limited to: in press release, in court documents, during judicial hearings, or during other public forums or proceedings. Accordingly, the [police department] agrees to the following conditions in connection with its purchase and use of the Harris Corporation equipment/technology:

* * *

The [police department] [prosecutor’s office] shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State’s case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI.

* * *

While the City will not voluntarily disclose any Protected Product, in the event that the city receives a Public Records request from a third party relating to any Protected Product, or other information Harris deems confidential, the City will notify Harris of such a request and allow Harris to challenge any such request in court. The City will not take a position with respect to the release of such material, beyond its contractual duties, but will assist Harris in any such challenge.
Chapter 6

Connecting to Our Future: The Digital Livable City

Mary Beth Henry
Portland, Oregon

David Olson
Cableworks
Portland, Oregon

Contents

Connecting to Our Future: The Digital Livable City ........................................ 6–1
Abstract ........................................................................................................... 6–1
Introduction ..................................................................................................... 6–2
Planning for Your Broadband Future: Role of Local Government in Facilitating
Broadband Infrastructure .................................................................................. 6–2
The Changing Nature of Work Relies on Broadband Infrastructure ................. 6–5
Responsive (Smart) City and Playable Cities ..................................................... 6–5
What Is Digital Equity? ..................................................................................... 6–8
Why Create a Local Digital Equity Action Plan? ............................................. 6–9
Youth and the Internet ...................................................................................... 6–9
Older Adults and the Internet ......................................................................... 6–10
Conclusion ....................................................................................................... 6–10
Endnotes .......................................................................................................... 6–11
Bibliography .................................................................................................... 6–12

U.S. Telecom Ass’n v. Fed Commc’ns Comm’n (D.C. Cir., 2016) ....................... 6–15
Abstract

Urban planners typically focus on the built environment with a goal of creating connected, healthy, prosperous cities. They should also pay heed to the importance of the Internet. The Internet is just as vital a part of a city’s infrastructure as its roads, bridges, and electrical grid. Access to the Internet has become essential for full participation in society, yet many communities are not integrating broadband Internet infrastructure, access, and training into local plans: many cities and their citizens are on the wrong side of the digital divide, which separates those people who have access, devices, and digital skills from those that do not.

Ubiquitous, affordable high speed Internet via fiber and wireless can be transformative in creating the healthy, equitable, responsive cities of the future. For example, high speed Internet is a necessary prerequisite for telework and telehealth applications. Both benefit the environment and reduce greenhouse gases by lowering auto emissions. Telework can reduce construction demand for office space, road maintenance and related energy use. Telehealth patients can consult with specialists using high definition interactive video from their own homes. These and a wide range of other broadband-based applications have enormous potential to improve the sustainability, wealth, and health of cities in the future.

Planners must also be aware of potential negative impacts of the Internet such as a more sedentary lifestyle and isolation due to too much time in front of the computer screen. Incorporating flexible communal gathering spaces in affordable housing complexes that can be used as Internet access and training classrooms and then transformed for other social activities like an exercise class can help address both issues. Given the increasingly digital world in which we live the benefits of being connected outweigh the drawbacks.

However, unless local communities develop targeted, collaborative solutions to address the digital divide, income disparities will continue to grow. It is going to take the whole community – providers, planners, architects, elected officials, non-profits and citizenry to address the digital divide. Author Jane Jacobs argued that “cities have the capability of providing something for everybody, only because, and only when, they are created by everybody”. Digital infrastructure will play an increasingly important role in creating more livable cities and combating climate change but only if everyone has the opportunity to participate in the digital age.

This paper will explore strategies by which localities can provide or facilitate state-of-the-art broadband expansion to meet future needs, how the Internet is changing the nature of work, the importance of being a responsive (smart) city, observations on youth and the Internet, older adults and the Internet, and the necessity of addressing digital equity at the local level to ensure that the entire community has affordable Internet, devices and digital literacy to provide everyone with the opportunity to benefit in the digital age.

“If you don’t at least try to think digitally, the digital economy will disrupt you. It will drain your town of young people and leave your business in the dust. If you don’t have access to the technology, or if you don’t know how to use it, it’s similar to not being able to read and write.”

Roberto Gallardo

“Everything wants to be connected” Sheldon Renan

Introduction

Ubiquitous, affordable high speed Internet via fiber and wireless can be transformative in creating the healthy, equitable, responsive city of the future. For example, high speed Internet is a necessary prerequisite for telework and telehealth applications. Both benefit the environment and reduce greenhouse gases by lowering auto emissions. Telework can reduce construction demand for office space, road maintenance and related energy use. Telehealth patients can consult with specialists using high definition interactive video from their own homes. These and a wide range of other broadband-based applications have enormous potential to improve the sustainability, wealth, and health of cities in the future. Yet affordable, state-of—the art broadband is not a given in every community. Communities need to develop local broadband strategic plans that lay the foundation for understanding, embracing, creating and adapting to the digital economy. Broadband plans should define the values to ensure a safe, sustainable and equitable future with technology and connectivity as pervasive forces. By way of example, Portland, Oregon developed a community-driven broadband strategic plan focused on ensuring ubiquitous wireless and wireline connectivity, critical infrastructure to facilitating the use of technology and data to address urban challenges as well as digital equity.

Peter Hirschberg, Chair of the City Innovate Foundation, says that the digital livable city is a city that “engages with citizens in acts of co-creation…in acts of democracy, care and ownership of the city.”

Planning for Your Broadband Future: Role of Local Government in Facilitating Broadband Infrastructure

Are you broadband ready?

Communities in many nations recognize the benefits that stem from high speed broadband networks and have made tremendous progress in recent years in fostering their deployment. Nonetheless, many challenges remain in terms of how to enhance and expand these networks to meet the growing demands of an increasingly digital economy and society.

This paper focuses on two models: public networks and public-private partnerships or “3P” networks where the risk of deployment is shared between the public and private sectors.

Public Network/Anchor Institution

Although private investments have been the overwhelming source of finance for high speed networks, municipal networks have been successfully deployed in the US and Europe.
Every network deployment involves a number of components – design, constructing, operating, marketing, and financing, to name the major ones. The question is: what role should the city play in the project? As cities approach this question, the basic trade-off involves risk and control.

Cities can assume the whole risk by serving residents with a public network. Another option is for local governments to directly build or finance a network that connects the anchor institutions such as libraries, schools, and local government offices, but not serve the public directly. SandyNet in Sandy, Oregon, is an example of a local government-run network that serves the entire City. SandyNet’s story is told in this video produced by The Institute for Local Self Reliance: [http://muninetworks.org/content/gig-city-sandy-home-60-gig](http://muninetworks.org/content/gig-city-sandy-home-60-gig). An example of a publicly-owned anchor institution network is IRNE, established in 2000 by the City of Portland to serve government offices.

**Public Private Partnership**

Another model is the public private partnership (3P) where risk and control are shared. One model has the City building and owning the infrastructure with services over the network being provided by the private sector. This is the model in Westminster, MD, which partnered with a private company, TING.

**Private: Incent a Competitive Broadband Market**

The strategies that local governments can pursue to advance private broadband deployment fall into three general categories: (1) facilitating access to key assets such as fiber, conduit, utility poles and real estate; (2) making useful information available; and/or (3) streamlining, accelerating and/or publicizing essential local processes.

**Access to key assets**

All local governments own or manage real estate assets of varying value. Policies like “dig once” and “one touch make ready” for pole attachments facilitate deployment.

“Dig once” policies require that whenever a project involves digging up streets, fiber should also be installed. For both political and administrative reasons, this is easier said than done—cities often lack full knowledge of all ongoing or planned projects, and complying with the policy requires funding, coordination and knowledgeable staff both in connection with the applicant and the government licensing entity. But such policies are significant cost-savers and constitute an investment in a city’s future. Such policies also protect roads and sidewalks from frequent, life-shortening cuts and minimize traffic and other disruption from utility construction. Before a
pole may be used for a new attachment, ‘make-ready’ work is usually needed — the existing attachments on the pole have to be rearranged so that it is ready for a new attacher. Often times, there are multiple attachments on the pole already (e.g., telecommunications, cable etc.), and, currently each is moved sequentially — which can create delays and multiple disruptions in a neighborhood. In the case of “one touch make-ready,” companies that own poles agree on one or more common contractors that could move existing attachments on a pole (‘make ready’ work), allowing a single crew to move all attachments on a pole on a single visit, rather than sending in a unique crew to move each attachment sequentially. Sending in separate crews is time-consuming and disruptive to local communities and municipal governments. One-touch make-ready polices would ease this burden.xiii

Access to Buildings

One significant barrier to new network providers is the need to gain entry into a building or development. Cities can improve services to residents and businesses if City code or other applicable requirements create an incentive for developers to build additional pathways from the public rights-of-way to a demarcation point in the building, and then requires internal, standards-compliant building cabling or cable pathways in new construction or major renovations.xiv

Make data available wherever possible

Many communities have robust GIS data including everything from centerlines of streets to home locations to demographics to city-owned fiber, conduit and poles. Making GIS data available to potential partners’ localities can enable providers to consider leasing public fiber and conduit as part of their network designs and business plans. Access to this essential information can both attract and speed new construction by private partners, while enabling the community to meet its goals for new, better broadband networks—and potentially to realize revenues for use of the assets.

Streamline and publicize procedures and timeframes for permitting and inspections

Efficient and streamlined processes can be one way in which broadband projects may proceed expeditiously, whether the entity building the broadband facilities is the locality itself or a private entity that seeks to deliver services to the community. All processes required for a broadband project should be formalized and well publicized. These range from rights-of-way access to permitting to final inspection and approval. Full transparency about these processes is the single most effective means by which to enable the communications industry to expeditiously plan and deploy networks.xv

Public Wi-Fi

Communities that provide or facilitate free WiFi in schools, libraries and other local government buildings are becoming more common. Free WiFi can be implemented incrementally, over time to spread the cost. Approximately 90% of City of Portland buildings have free WiFi. WiFi can also be expanded outward from the schools and libraries to provide connectivity for the surrounding neighborhoods.
The Changing Nature of Work Relies on Broadband Infrastructure

“Work in the future will be organized in ways that are far more decentralized.”xvi Work is no longer confined to a specific time and place. Networked Internet (including mobile) technology blurs the lines between work and home and between work and personal life. Tens of millions of people now work at home offices, telecommute or participate in “virtual companies” whose workers are scattered across the country or the globe. Many others work for startup firms in improvised settings. Open platforms for the “crowdsourcing” of work mean that work is becoming an activity that can occur anywhere, and at any time. The implications of this transformation affect our urban architecture (Who will occupy high-rise buildings?), tax structure (What is the correct structure for taxing business when its location is on the Internet, not the City) and our economic development strategies (How can leaders attract companies to locate in their city, if they are in fact virtual rather than physical?)

As mobile and wireline broadband becomes essential for daily life, more people participate in an information-driven economy, more and more people will not go to work, but the work will go to the people – wherever they might be, including home. This has already led to a decreased need for office space. Cisco Systems found that it needed 40% less office space per employee because of broadband-based tele-work and collaboration tools. There was also a significant reduction in energy use and greenhouse gases.xvii Urban policy must adapt to this new world and urban planners must re-think the assumptions that guided a society where work, home and shops were apart.

Work, even in large organizations, is increasingly dispersed and decentralized among people who connect by broadband networks. We are now in an era where people are able to work from anywhere and be paid well. So for those people, the question is not necessarily where the jobs are, but where the quality of life is highest for them as long as there is good internet access.

Responsive (Smart) City & Playable Cities

What is a responsive city? According to the International Telecommunications Union (ITU) “A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects.”xviii

Anthony Townsend goes a step further asserting that we need to empower ourselves to build future cities organically, from the bottom up, and do it in time to save ourselves from climate change. He goes on to say that the smartest city in the world is the one you live in…if that’s not worth fighting for…what is.xix

What sets a responsive city apart is that it intentionally collects and uses better data and fewer resources and empowers residents with information and resources to improve their quality of life.xx Open data and equity are key components of a responsive city.xxxi Open data is data that can be freely used, re-used and redistributed by anyone - subject only, at most, to the requirement to attribute and share alike.xxxii The underpinning of the responsive city is that
individuals can monitor how their actions impact their environment in real time and make decisions accordingly.

Some “responsive” city initiatives from Portland, Oregon:

- **Vision Zero** - Originating in Sweden in the 1990’s, VisionZero seeks to reduce traffic fatalities to zero. Achieving Vision Zero requires a comprehensive approach that engages diverse partners and utilizes a wide range of education, enforcement, as well as digital and engineering strategies.xxiii

- **Portland’s new bike share program**, called BikeTown, is a collaborative partnership with Nike. Nike is providing some funding and will oversee the design and branding of the system’s logo, stations and digital presence.xxiv

- **Ubiquitous Mobility Portland or UB Mobile PDX** envisions a single all-purpose “marketplace” that would let smartphone users find a BikeTown bike, hop on a Tri-Met bus, rent a bike through Spinlister or call a Lyft driver or whatever. The app could also integrate parking payments and even a potential pay-per-mile fee. The app would let users weigh their mobility options based on personal needs such as cost, travel time and other factors like carbon emissions. The concept is to create access to the myriad transportation options that is so integrated that everyone can easily plug into it.xxv

*Using “smart city” data to prove Jane Jacobs’ points*

In the Death and Life of Great Italian Cities: A Mobile Phone Data Perspective researchers gathered data from mobile phones to empirically test Jacobs’ concepts of the factors necessary for a city to be “livable”.xxvi The research extracted human activity from mobile phone data, collected land use and socio-economic data from the Italian Census and Open Street Map and tested Jacob’s theories in six Italian cities. The empirical data supports Jacobs’ assertions of the factors that must be present for a city to be livable.

What is a playable city? A playable city takes the responsive city concept a step further, inviting residents and visitors to interact with embedded technology and connectivity in a playful way. A playable city requires the smart technology that is integrated in a smart city environment. Sensors, displays, smart tangible objects, and wearables, can be used to improve the efficiency of city management (traffic, public transport, security, public events, etc.), but they can also introduce playful elements. A city without smart technology embedded in its urban environment cannot offer people playful interactions with streets, buildings, street furniture, traffic, public art, and public events.xxvii

An example of the playable city in Portland, OR is the Tilikum Crossing, the largest car-free bridge in the U.S., which features lights that change color and timing based on changes in the Willamette's river speed, height and water temperature. It is a way for people in Portland to connect more with the river.xxviii The data is collected by a U.S. Geological Survey river monitor.
These murals of “bots” below beckon passersby to take a photo and upload the photo with the answer to the question to the artist’s website. This is another example of playful public art and digital media. xxix

Richard Florida writing in The Creative Class found that young people seek vibrant cultural opportunities, recreational institutions, walkable streets and transit. One important addition in today’s digital world is the need for ubiquitous, affordable high speed Internet. The concept of a playful city is attractive to young people who are seeking places to live, work, play and stay.
What is Digital Equity?

In 2016, many of us take our access to high-speed Internet and our use of digital tools for granted. We have a computer on our desks at work, a smartphone in our hands and a laptop or tablet in our briefcase or backpack. We grumble about the price, but we expect and pay for speedy broadband Internet connections that make it possible to work online efficiently and effectively.

But what if you couldn’t afford or didn’t know how to use your device and your high-speed Internet connection? How would you apply for a job, find housing, get financial aid for college, communicate with your doctor or your child’s school, do your homework or file your tax return? Too many people in our community are still excluded by poverty, language barriers, disability and a lack of training from the digital world the rest of us now inhabit.

The National Digital Inclusion Alliance defines digital equity as everyone having “daily access to the Internet, at speeds, quality and capacity necessary to accomplish common tasks, with digital skills necessary to fully participate online, and whenever possible on a personal device and home network.”

The social and external cost of digital exclusion is great. Without access, full participation in nearly every aspect of American society — from economic success and educational achievement, to positive health outcomes and civic engagement — is compromised.
Why Create a Local Digital Equity Action Plan?

Local communities should develop targeted, collaborative solutions to address the digital divide or income disparities will continue to grow. It is going to take the whole community – providers, planners, architects, elected officials, non-profits, and citizenry to address the digital divide. Author Jane Jacobs argued that “cities have the capability of providing something for everybody, only because, and only when, they are created by everybody”. One way to start addressing digital equity is to gather local data on barriers to adoption. Portland, Oregon conducted five focus groups with historically underrepresented populations (Spanish, Chinese and Vietnamese speakers, people with hearing disabilities and African Americans). xxxii Digital equity action plans target access and adoption gaps for excluded and disadvantaged communities, specifically people living in poverty, older adults, communities of color, people with disabilities, and those with limited English proficiency.

The Internet provides access to jobs, healthcare, education, banking, culture and civic engagement. The Internet is a top resource for many of today’s job hunters: Among Americans who have looked for work in the last two years, 79% utilized online resources in their most recent job search and 34% say these online resources were the most important tool available to them.xxxiii

It is important to remember, however, that technology is a just a tool; it amplifies existing human capacities. Technology can make things better when there is a deliberate intention—economically, politically, culturally—to push against the gradient of inequality.xxxiv

Youth and the Internet

The Organization for Economic Co-operation and Development (OECD) research shows that too much computer and Internet use – particularly unsupervised and unstructured – crowds out real learning, socializing and intellectual development in children.xxxv Certainly an unhealthy relationship with technology can have negative consequences. However, research from danah boyd’s book, It’s Complicated: The Social Lives of Networked Teens, shows that most teenagers go online to connect to the people in their community. Some older adults believe that their own childhoods were better than the ones young people experience in today’s digital world associating the rise of digital technology with decline. The research presented by Danah Boyd suggests that the opposite is often true. What is different today is that teens’ use of social media is public by default and private through major effort. Facebook and Twitter are providing teens with new opportunities to participate in public life which is what concerns many anxious adults.

Many public spaces where adults gather, such as bars and clubs are not available to teens. Teens have fewer places to be together in public than they once did. Planners should include teens in creating the vision of the future city. Teens would rather meet up in person, but heavily scheduled daily lives and lack of physical mobility makes it challenging. The Internet mirrors, magnifies, and makes more visible the good, the bad, and the ugly of daily life.
Older Adults and the Internet

In an era when everything, from personal health records to nursing home quality ratings, is online and the best way to stay in touch with grandchildren may involve Facetime or texting, internet connectivity and digital literacy are essential. Yet many older adults, especially those with low incomes, are not online. Older adults may have additional challenges such as physical limitations or cognitive impairment that serve as barriers to adoption. There are two model programs that are blazing the trail for older adult connectivity. Older Adult Technology Services (OATS) uses technology to empower older adults to live successful, independent, connected lives. The many program offerings are holistic addressing the unique needs of older adults. The CareWheels program empowers people to age in place with a variety of technology/services tailored to individual needs.

In a study to examine how Internet use affects social isolation and loneliness of older adults in assisted and independent living communities, researchers found that using the Internet may be beneficial for decreasing loneliness and increasing social contact among older adults. Older adults need access, devices and age-appropriate training to realize the benefits of connectivity.

Conclusion

The full potential of the digital livable city will not be realized until cities assume a leadership role in ensuring ubiquitous, state of the art broadband throughout the community and provide a pathway for everyone to be connected, have a device and understand how to engage in the digital world. Some cities are moving in a deliberative fashion to design their digital future. The digital economy is helping to create new attitudes about the role of local government and leadership that aims to facilitate and empower, not dictate and control residents. However until everyone is online, a collaborative, citizen-engaged creation of community in the digital age will not be realized.

Local officials need to convene a diverse set of stakeholders, be transparent and inclusive, listen and engage, and then follow-through with implementation. Broadband is critical infrastructure. Demand for broadband is growing. Ubiquitous affordable access to fiber and wireless Internet as well as devices and culturally-specific training should be part of a community-developed broadband plan.

One thing that hasn’t changed in the digital era is the need for urban policy to ensure cultural and educational opportunities as well as inviting gathering places for people to meet face to face so that cities are vibrant areas to live. Even in a digital world research shows that in-person interactions are an essential part of being human. Sherry Turkle in her book Reclaiming Conversation demonstrates that children develop better, students learn better and employees perform better when their role models take time for in-person conversations.

Intelligent infrastructure can help make all the other infrastructure – roads, energy, water and waste – work better and operate in a greener way. Urban planners will need to understand how the design and form of the built environment will become dramatically changed by these
broadband transformations. Urban policy makers and urban planners must face the changing world and changing requirements on urban life that broadband networks will necessarily impose. In person social systems - community gathering places and engaged citizenry are vital to the successful transformation. CES Wood, one of Portland’s respected early leaders said, “Good citizens are the riches of a city.” That is as true or more so in the digital livable city.

ENDNOTES

i http://www.wired.com/2015/11/the-land-that-the-internet-forgot/
ii http://www.slideshare.net/srenan?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideview
iv http://csreports.aspeninstitute.org/Roundtable-on-Information-Technology/2015/report
v http://www.oecd-ilibrary.org/content/workingpaper/5jrqd7rvns3-en
vii http://www.ci.sandy.or.us/SandyNet/
viii http://www.portlandoregon.gov/revenue/article/394185
ix http://nextcenturycities.org/connecting-21st-century-communities-a-policy-agenda-for-broadband-stakeholders/
x http://www.westgov.com/373/FTTP
xiii http://nextcenturycities.org/2016/01/06/one-touch-make-ready-policies-the-dig-once-of-pole-attachments/
xvi http://www.aspeninstitute.org/publications/future-of-work
xvii http://www.pcworld.com/article/167503/cisco_promotes_telecommuting.html
xix https://placesjournal.org/article/smart-cities/?gclid=CjwKEAjw67SvBRC1m5zPv4GboAUSJAB6MJJkJPQaeAHW3p619YMFDXGApclaGpLJ -J-HqW0-K5JJ2xoC28Pw_wcB
xx Knox, Paul, Atlas of Cities
xxi Goldsmith, Stephen & Crawford, Susan, The Responsive City
xxii http://opendatahandbook.org/guide/en/what-is-open-data/
xxiii http://www.portlandoregon.gov/transportation/40390
xxiv http://www.portlandoregon.gov/transportation/article/562824
xxv https://www.portlandoregon.gov/transportation/article/564107
xxvi http://arxiv.org/abs/1603.04012
xxviii http://catchtheorange.com/#/tilikum
Bibliography


Cotton, Sheila, Anderson, William, McCullough, Brandi. Impact of Internet Use on Loneliness and Contact with Others among Older Adults: Cross-Sectional Analysis. JMIR Publications 2/2013


JLA Public Involvement. Digital Needs and Opportunities Report. Office for Community Technology 8/2015

Kane, Joseph and Tomer, Adi (Authors). Broadband Adoption Rates and Gaps in US Metropolitan Areas. Metropolitan Policy Program at Brookings. 12/2015

Kentaro Toyama, Global Computing: The Internet and Inequality: Is Universal access to the Internet a realistic method for addressing worldwide socioeconomic inequality? Communications of the ACM 4/2016


Kondepudi, Sekhar N. Shaping Smarter and More Sustainable Cities: Striving for sustainable development goals. International Telecommunication Union, 6/2015


Mölleryd, Bengt G. Development of High Speed Networks and the Role of Municipal Networks. Organisation of Economic Cooperation and Development. 11/2015


Office for Community Technology, City of Portland, OR. Connecting to our Future: Portland’s Broadband Strategic Plan. 9/2011


Open Knowledge. Open Data Handbook

Portland Office of Planning and Sustainability. Portland Plan. 4/2012


Smith, Aaron. Searching for Work in the Internet Era. PEW Research Center 11/2015

Smith, Aaron. Older Adults and Technology Use. PEW Research Center 4/2014

Townsend, Anthony. Smart Cities: What if the smart cities of the future are chock full of bugs? Places Journal, 10/2013
United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued December 4, 2015  Decided June 14, 2016
No. 15-1063

UNITED STATES TELECOM ASSOCIATION, ET AL.,
PETITIONERS

v.

FEDERAL COMMUNICATIONS COMMISSION AND UNITED STATES OF AMERICA,
RESPONDENTS

INDEPENDENT TELEPHONE & TELECOMMUNICATIONS ALLIANCE, ET AL.,
INTERVENORS


On Petitions for Review of an Order of the Federal Communications Commission

The following pages contain excerpts from the U.S. Telecom Ass’n v. Fed Commc’ns Comm’n (D.C. Cir., 2016) decision. You may access the entire document (184 pp.) using this link: http://tinyurl.com/TECH16-Ch3
Before: TATEL and SRINIVASAN, Circuit Judges, and WILLIAMS, Senior Circuit Judge.

Opinion for the Court filed by Circuit Judges TATEL and SRINIVASAN.

Opinion concurring in part and dissenting in part filed by Senior Circuit Judge WILLIAMS.

TATEL and SRINIVASAN, Circuit Judges: For the third time in seven years, we confront an effort by the Federal Communications Commission to compel internet openness—commonly known as net neutrality—the principle that broadband providers must treat all internet traffic the same
regardless of source. In our first decision, *Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010), we held that the Commission had failed to cite any statutory authority that would justify its order compelling a broadband provider to adhere to certain open internet practices. In response, relying on section 706 of the Telecommunications Act of 1996, the Commission issued an order imposing transparency, anti-blocking, and anti-discrimination requirements on broadband providers. In our second opinion, *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014), we held that section 706 gives the Commission authority to enact open internet rules. We nonetheless vacated the anti-blocking and anti-discrimination provisions because the Commission had chosen to classify broadband service as an information service under the Communications Act of 1934, which expressly prohibits the Commission from applying common carrier regulations to such services. The Commission then promulgated the order at issue in this case—the 2015 Open Internet Order—in which it reclassified broadband service as a telecommunications service, subject to common carrier regulation under Title II of the Communications Act. The Commission also exercised its statutory authority to forbear from applying many of Title II’s provisions to broadband service and promulgated five rules to promote internet openness. Three separate groups of petitioners, consisting primarily of broadband providers and their associations, challenge the Order, arguing that the Commission lacks statutory authority to reclassify broadband as a telecommunications service, that even if the Commission has such authority its decision was arbitrary and capricious, that the Commission impermissibly classified mobile broadband as a commercial mobile service, that the Commission impermissibly forbore from certain provisions of Title II, and that some of the rules violate the First Amendment. For the reasons set forth in this opinion, we deny the petitions for review.
VIII.

For the foregoing reasons, we deny the petitions for review.

So ordered.
WILLIAMS, Senior Circuit Judge, concurring in part and dissenting in part: I agree with much of the majority opinion but am constrained to dissent. In my view the Commission’s Order must be vacated for three reasons:

I. The Commission’s justification of its switch in classification of broadband from a Title I information service to a Title II telecommunications service fails for want of reasoned decisionmaking. (a) Its assessment of broadband providers’ reliance on the now-abandoned classification disregards the record, in violation of its obligation under F.C.C. v. Fox Television Stations, Inc., 556 U.S. 502, 515 (2009). Furthermore, the Commission relied on explanations contrary to the record before it and failed to consider issues critical to its conclusion. Motor Vehicles Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983). (b) To the extent that the Commission relied on changed factual circumstances, its assertions of change are weak at best and linked to the Commission’s change of policy by only the barest of threads. (c) To the extent that the Commission justified the switch on the basis of new policy perceptions, its explanation of the policy is watery thin and self-contradictory.

II. The Commission has erected its regulatory scheme on two statutory sections that would be brought into play by reclassification (if reclassification were supported by reasoned decisionmaking), but the two statutes do not justify the rules the Commission has adopted.

Application of Title II gives the Commission authority to apply § 201(b) of the Communications Act, 47 U.S.C. § 201(b). The Commission invokes a new interpretation of § 201 to sustain its ban on paid prioritization. But it has failed to offer a reasonable basis for that interpretation. Absent such a basis, the ban is not in accordance with law. 5 U.S.C. § 706(2)(A) & (C).
Application of Title II also removes an obstacle to most of the Commission’s reliance on § 706 of the Telecommunications Act of 1996, 47 U.S.C. § 1302, namely any rules that have the effect of treating the subject firms as common carriers. See Verizon Communications Inc. v. Federal Communications Commission, 740 F.3d 623, 650 (2014). But the limits of § 706 itself render it inadequate to justify the ban on paid prioritization and kindred rules.

I discuss § 201(b) and § 706 in subparts A and B of part II.

III. The Commission’s decision to forbear from enforcing a wide array of Title II’s provisions is based on premises inconsistent with its reclassification of broadband. Its explicit refusal to take a stand on whether broadband providers (either as a group or in particular instances) may have market power manifests not only its doubt as to whether it could sustain any such finding but also its pursuit of a “Now you see it, now you don’t” strategy. The Commission invokes something very like market power to justify its broad imposition of regulatory burdens, but then finesses the issue of market power in justifying forbearance.

Many of these issues are closely interlocked, making it hard to pursue a clear expository path. Most particularly, the best place for examining the Commission’s explanation of the jewel in its crown—its ban on paid prioritization—is in discussion of its new interpretation of 47 U.S.C. § 201. But that explanation is important for understanding the Commission’s failure to meet its obligations under Fox Television, above all the obligation to explain why such a ban promotes the “virtuous cycle,” which (as the majority observes) is the primary justification for reclassification under Title II. Thus a discussion critical to part I of this opinion is
deferred to part II. I ask the reader’s indulgence for any resulting confusion.

* * *
* * *

The ultimate irony of the Commission’s unreasoned patchwork is that, refusing to inquire into competitive conditions, it shunts broadband service onto the legal track suited to natural monopolies. Because that track provides little economic space for new firms seeking market entry or relatively small firms seeking expansion through innovations in business models or in technology, the Commission’s decision has a decent chance of bringing about the conditions under which some (but by no means all) of its actions could be grounded—the prevalence of incurable monopoly.

I would vacate the Order.
Chapter 7

Self-Driving Vehicle Technology, Policy, and Liability—Presentation Slides

Richard Lazar
Techolicy
Portland, Oregon

Josh Schoonmaker
Director of Business Development
Tozny
Portland, Oregon
What is a Fully Self-Driving Vehicle?

- A motor vehicle operated solely by software and hardware rather than a person (i.e., technology-driven)
- Sensors – radar, LIDAR, cameras, odometry and GPS – dynamically detect a vehicle’s environment and location
- Dedicated short-range communications capabilities may connect and communicate with other vehicles (vehicle-to-vehicle communications, or “V2V”) and technology-enabled roads, signals, signs, obstacles, etc. (vehicle-to-infrastructure communications, or “V2I”), to gain additional situational awareness
- Software algorithms interpret sensor and communications inputs and exert control over the vehicle’s throttle, braking and steering systems to transport occupants to their destinations
Continuum of Automated Driving Levels: SAE 0-5

Current State of U.S. AV Public Policy

Autonomous Vehicle Laws, Regulations and Legislation as of October 2016

<table>
<thead>
<tr>
<th>Laws and Regulations</th>
<th>Number of Jurisdictions with AV-related laws</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of jurisdictions with AV-related regulations</td>
<td>2</td>
</tr>
<tr>
<td>Legislative and Regulatory Activity</td>
<td>Number of jurisdictions with legislative activity</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Number of bills introduced this legislative session</td>
<td>75</td>
</tr>
<tr>
<td>Bill activity by status</td>
<td>Pending</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Enacted</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Failed</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Number of jurisdictions with pending regulations</td>
<td>2</td>
</tr>
</tbody>
</table>
Current State of U.S. AV Public Policy

- Preemption
- Liability and Risk
- AV PUBLIC POLICY FRAMEWORK TOPICS & ISSUES EXPRESSED OR IMPLICITLY FOCUSED ON IN CURRENT APPROACHES:
  - State Frameworks Very Widely Vary

NHTSA & Government’s Role in AV Policy Development

B. The Federal and State Roles:
The division of regulatory responsibility for motor vehicle operation between Federal and State authorities is clear. NHTSA responsibilities include:

- Setting FMVSS for new motor vehicles and motor vehicle equipment to which manufacturers must certify compliance before they sell their vehicles.¹⁰
- Enforcing compliance with the FMVSS.
- Investigating and managing the recall and remedy of non-compliances and safety-related motor vehicle defects and recalls on a nationwide basis.
- Communicating with and educating the public about motor vehicle safety issues.
- Issuing guidance for vehicle and equipment manufacturers to follow, such as the Vehicle Performance Guidance for AVs presented in this Policy.

States’ responsibilities include other aspects of motor vehicle regulations:

- Licensing (human) drivers and registering motor vehicles in their jurisdictions.
- Enacting and enforcing traffic laws and regulations.
- Conducting safety inspections, where States choose to do so, and
- Regulating motor vehicle insurance and liability.

No meaningful role defined for local government
The Liability Conundrum

The Lawyer Contribution

- Current state of the law + business impacts
- Litigation
- Regulatory compliance
- Business strategy
- Fundraising and M&A
- Insurance and risk management
- Data privacy and security
- Lobbying and advocacy
TYPES OF DATA

USER RELATED
- Personal ID (PII)
- Location (LBS)
- Location Derived (LBS)
- Pass Thru (WiFi)

DIRECT SURVEILLANCE
- Video
- Audio
- Surveillance Derived

STAKEHOLDERS

INDIVIDUALS
- Users
- Criminals

BUSINESSES
- MOD Fleet Operators
- 3rd Party Data Consumers
- Insurance

THE VEHICLE
- Vehicle Manufacturers
- Control System Developers
- Network Providers
- App Developers
- Maintenance & Repair

GOVERNMENT
- Regulatory Bodies
- Research
- Enforcement
PRIVACY-BY-DESIGN

PRIVACY-BY-DESIGN PRINCIPLES

1. Proactive not Reactive
2. Privacy as Default Setting
3. Privacy Embedded into Design
4. Full Functionality
5. End-to-End Security
6. Visibility & Transparency
7. Respect for User Privacy
8. Keep it User-Centric

PRIVACY-BY-DESIGN

FTC PRINCIPLES OF PRIVACY

1. Data Security
   Provide reasonable security for consumer data
2. Reasonable Collection Limitation
   Limit collection of data
3. Sound Data Retention
   Implement reasonable data retention and disposal
4. Accuracy
   Maintain reasonable accuracy of consumers’ data
5. Consumer Transparency
   Transparency and Simplified Consumer Choice
RELEVANT LEGAL PRECEDENCE

REASONABLE EXPECTATION

SURVEILLANCE

EVENT DATA RECORDER (EDR)

MOBILE DEVICE DATA

PERSONAL AUTONOMY

THANKS FOR SHARING YOUR TIME

ANY QUESTIONS?

Contact:
Richard A. Lazar, Principal
AV Insights, LLC
(503) 702-0635
richard@av-insights.com

Copyright © 2016 AV Insights, LLC