Robert L. Aldridge, Chartered
Attorney at Law
1209 North Eighth Street
Boise, Idaho 83702-4297
Telephone: (208) 336-9880
Fax: (208) 336-9882
State Bar No. 1296
Cell phone: (208) 631-2481
email: Bob@RLAldridgeLaw.com

TALKING POINTS
SB 1303, as amended

1. General Subject of Bill

This bill is referred to as the Revised Uniform Fiduciary Access to Digital Assets Act. This bill deals only with digital assets: examples being email; Facebook and other social media; online accounts for banking and investing; the Cloud; LinkedIn; photographs; ancestry accounts; Instagram and Twitter; online services such as Amazon and eBay; access to movies; and, many other digital accounts and property. The list is almost endless. The bill modernizes the law as to access to such digital assets by fiduciaries. Fiduciaries are persons entrusted with the legal authority to manage another person's property and with a duty to act in that person's best interest. This bill addresses four common types of fiduciaries:

1. Personal Representatives (also called Executors or Administrators) for a deceased person's estate;
2. Court-appointed guardians or conservators for a living protected person's estate;
3. Agents appointed under powers of attorney; and,
4. Trustees.

2. Existing Problem

A generation ago, our mail was delivered in person, photos were kept in albums, documents were kept in file cabinets, and money was deposited in the local bank. Now the nature of our property and our methods of communication have changed dramatically.

In general, a person's digital property and electronic communications are collectively referred to as "digital assets". The companies that store those assets are called "custodians". Access to digital assets is usually governed by a "terms of service" agreement rather than by property law.

In Idaho, and nation-wide, digital assets present unusual problems.

- The first is that with a very high percentage of people having such digital assets, and many of those assets containing vital information, both personal and business,

those assets may have real value, both monetary and sentimental. Access to those assets may be critical to continuing a business for example, or for carrying out the estate plan of a decedent. But such assets are almost always protected by passwords and restrictive terms of service agreements with the provider.

- But at the same time, digital assets present unique privacy concerns. Private communications like email and social media conversations are protected by federal privacy law. The person holding the account may or may not want a fiduciary to have access to digital assets, or may want such access restricted in various ways.

- Current Idaho law refers to digital assets only briefly and without any detail or enforceable provisions.

3. Solution in Bill

This bill is the result of years of work on the national level involving a wide cross section of the persons and entities involved in digital assets. Providers, privacy groups, consumer groups, organizations representing of fiduciaries, groups such as the Motion Picture Association and many others concerned with copyright and other such issues, and many many more. This bill is a consensus of those groups on a workable and practical solution to the many problems posed by digital assets.

In its most simple terms, this bill is a balancing of the need for fiduciaries to have access to digital assets, the need for the privacy of the holder of the account to be kept unless the holder is willing to have the account be available, and protection for the providers of the accounts.

Specifically, this bill strikes that balance by:

a. Giving the holder of the account control. The holder is allowed to specify whether their digital assets should be preserved, distributed to heirs, or destroyed. There is a three tiered system of priorities for how consent is given:

1. If the custodian provides an on-line tool, separate from the general terms of service, that tool allows the user either to name another person (who may be a fiduciary or may be a "designated recipient") to have access to the user's digital assets or to direct the custodian to delete the user's digital assets in the case or death or incapacity.

2. If there is no on-line tool, or the user declines to use the tool, the user can 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 on-line or in a traditional estate plan, the terms of service for the account will determine whether the

fiduciary may access the digital assets. If the terms of service do not address fiduciary access, the default rules of the bill apply. Those balance the user's privacy interests 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.

A. The "content of electronic communications" includes the subject line and body of email, text, and other messages between private parties. A fiduciary can never access the content of electronic communications with the user's consent.

B. The "catalogue of electronic communications" is the list of communications showing the addresses of the sender and the recipient and the date and time the message was sent. For example, this might allow the Personal Representative of an estate to determine that the decedent received a monthly email message from a particular bank or credit card company, and the Personal Representative can then contact that bank or credit company to obtain account information.

4. Some types of digital assets are not communications, but rather intangible personal property. This can include files stored in the "cloud", or photos on a photo-sharing web site. In dealing with those, the fiduciary is subject to the same fiduciary duties that apply to tangible assets. For example, the Persona Representative cannot publish the decedent's confidential communications or impersonate the decedent by sending emails from the decedent's account. Other laws or restrictions may also apply, such as copyright law, federal privacy acts, and the terms of service agreement.

b. Providing uniformity. Digital assets travel across state lines nearly instantaneously, and people are mobile, relocating often. It would be nearly impossible for a user or provider or estate planner to negotiate a maze of conflicting guidelines on access to digital assets.

c. Respecting privacy interests. As stated previously, private communications like email and social media conversations are protected by federal privacy law. This bill prevents companies that store communications from releasing them to fiduciaries unless the user consented to disclosure.

d. Recognizing the different types of fiduciaries that may need access - personal representatives of an estate, agents under powers of attorney, court appointed conservators, and trustees. This removes any confusion about whether a trustee, for example, is covered by the act.

e. Requiring clear proof of authority. Generally, fiduciaries must provide proof of their authority by a certified documents.

f. Recognizing limits from federal law, such as the Copyright Act and the Electronics Communications Privacy Act.

g. Protecting custodians of digital assets that comply with a fiduciary's apparently authorized request for access, by giving them immunity so long as they act reasonably and in good faith.

4. Possible Questions

a. What were the amendments? The amendments were very simple. It was recognized after the uniform act was approved and this bill prepared, that the act applied to both fiduciaries and to "designated recipients", duly defined at the beginning of the bill - persons named to have access to the account who were not acting as a fiduciary. However, "designated recipients" were not always clearly referenced in a few parts of the bill. Therefore, the bill was amended to also name the "designated recipient" directly in a few places in the bill.

b. What about the FBI vs. Apple controversy? That is a criminal prosecution, not a civil proceeding, so the legal issue are very different. However, the Electronic Communications Privacy Act of 1986 does apply to both civil and criminal proceedings. Therefore, access to the content of electronic communications is barred. There is an exception for law enforcement agencies with a warrant or court order. In fact, the FBI has already obtained much of the information from the shooter's email service provider, and all of the phone's backed up data from Apple. The dispute arose when the FBI was unable to access other data on the phone which had not been backed up and was not available from any other source.

There obviously was no consent to release of the information by the shooter, another possible exception to the Privacy Act.

The real problem is that even if a provider is permitted by law to release private data, encryption may prevent release. Apple's latest generation of the iPhone lets a user choose a 4 digit pass-code to access the main screen. Apple does not record that pass-code and without the pass-code, the phone is useless. Additionally, as an added security feature on the iPhone, after ten incorrect attempts to enter a pass-code, the phone will automatically and permanently erase its data. This defeats "cracking" the pass-code by generating millions of pass-codes rapidly until the correct pass-code is found, a technique often used both by hackers and by law enforcement.

The FBI wants Apple to write a program that defeats automatic erasure and allows the FBI to try unlimited numbers of pass-codes. Apple has appealed on the grounds

that creating such a feature would endanger the private data of all iPhone users and would be subject to abuse.

The real lesson of the FBI-Apple battle is that access to data, even if legally available, may be worthless without additional information from the user - the user name and the password. So, if a person wants their fiduciaries to have access to their digital assets, they should provide in some manner a list of the user names and passwords for their digital assets, perhaps by having them in a list only available to the fiduciary when needed. Estate planners are working on such methods. Conversely, if the user does not want access to be given, the failure to provide that information to the fiduciary is an added layer of protection.

5. Fiscal Impact

None. This may lower court involvement in such cases, creating a positive fiscal impact.