AN ESTATE DILEMMA - INACCESSIBLE ASSETS HIDING BEHIND PASSWORDS AND ENCRYPTION

DOUGLAS J HENDERSON
An Estate Dilemma - Inaccessible Assets Hiding Behind Passwords and Encryption

Douglas J. Henderson
Contents
Introduction..................................................................................................................................... 3
The Public is increasingly Adopting Password Protection and Encryption ................................... 3
Encryption Explained.................................................................................................................. 4
   An Explanation of the Difference between Binary System Encoding and Encryption .......... 5
The Role of Law in Increasing Password Protection and Data Encryption............................... 6
   The Two Umbrella Encryption Methodologies – Symmetric and Asymmetric ................ 8
   An Example of Symmetric Encryption .................................................................................. 8
   An Example of Asymmetric Encryption ................................................................................ 10
The Password Protected Digital Device ....................................................................................... 11
   Where Initial Question Answers Lead the Responsible Party .............................................. 11
The Computer Fraud and Abuse Act (CFAA) ........................................................................... 12
Solutions to Accessing a Password Protected Computer .............................................................. 14
Types of Data Possible on the Computer (Including Assets and Directions to Assets) .......... 15
   Encrypted Files ......................................................................................................................... 15
      Financial Data Covered by the Gramm-Leach-Bliley (GLB) Act .................................. 15
      HIPAA Covered Data ........................................................................................................... 17
   Unencrypted Files ...................................................................................................................... 17
      Intellectual Property .............................................................................................................. 17
      Spreadsheet and Accounting Files ..................................................................................... 18
      Adult or Child Pornography .................................................................................................. 18
      Computer History, Registry, and Temporary Files .............................................................. 19
Internet Content ............................................................................................................................ 19
   Access Limitations on Web Portals the Responsible Party Was Directed To .................. 20
      Terms of Service (ToS) ......................................................................................................... 20
   The Stored Communications Act ............................................................................................. 21
      An Example of How the SCA Can Be Used to Prohibit Access ...................................... 22
      An Example of How the SCA can Provide Protections ...................................................... 22
Cloud Computing ......................................................................................................................... 23
Conclusion .................................................................................................................................... 23
**Introduction**

Every person living in the modern world holds valuable assets, data, or information in digital mediums. Digital mediums include not only digital hardware storage mediums in personal possession (like external hard drives and internal hard drives within laptop and desktop computers, personal digital assistants, cell phones, and the like), but also those only accessible through a network. Because so much is held in digital mediums, when an individual dies or becomes incapacitated, another person must know how to access the incapacitated person’s digital assets and other important information (this person is known herein as the ‘Responsible Party’). There are potential barriers to accessing digital data, information, and online accounts, though, such as legal or contractual restrictions, password protection, and encryption. As a consequence, a Responsible Party seeking to properly perform his or her duties must know what to do with password protected and encrypted digital data in a way that 1) does not violate state or federal law, 2) efficiently and effectively gains possession of digital assets, 3) provides proper maintenance for all digital assets and liabilities, and 4) appropriately accumulates, returns, and distributes all assets and other information held behind password protection and encryption.

**The Public is Increasingly Adopting Password Protection and Encryption**

Computer hardware can now be purchased with built-in security measures,\(^1\) and stand-alone security software can be downloaded or purchased at little to no cost.\(^2\) Computer hardware with built-in security measures and encryption security software have the ability to provide impenetrable security regimes. For instance, Seagate Technology, LLC, a well-known provider of computer hard drives, currently sells a hard drive called the BlackArmor. This hard drive is

---


preset to have no password protection (the simplest, least secure form of security protection), but can be set to utilize an industry standard method of encryption known AES cryptographic algorithm (See below for an explanation of AES cryptography). In 2008 Seagate stated that if it is assumed there were 7 billion people, each with 10 computers a piece, and assuming each computer could guess 1 billion passwords per second, it would take 77 septillion years\textsuperscript{3} to guess a 128-bit password\textsuperscript{4} if the password can be guessed after 50\% of the total number of possible passwords have been guessed.\textsuperscript{5}

**Encryption Explained**

Encryption can be defined as the scrambling of readable, usable data and information, into something that is configured in such a way that it cannot be de-scrambled without input from the party that originally encrypted the data or information.\textsuperscript{6} Today’s encryption techniques work so well that they can make the data and information behind the encryption methodology inaccessible unless the creator decrypts it or has left behind a key to allow another party to do so.

Techniques of encryption have been used since warfare became organized and merchant market systems came into existence. As time passed, encryption techniques had to increase in complexity in order to achieve their primary purpose – to make messages, data, and information unreadable and irretrievable by those it wasn’t intended. Two thousand five hundred years ago, the Greeks and Spartans used techniques such as scytale, whereby a sheet of papyrus was wrapped around a staff down the length of the staff and could only be read when re-wrapped

---

\textsuperscript{3} 77 septillion is \num{770000000000000000000000000000000000000}.

\textsuperscript{4} Posting of Jim D. Lamm, to http://www.digitalpassing.com/page/5/ (Feb. 8, 2011).


around a staff of exactly the same diameter,\textsuperscript{7} to achieve the purpose of data encryption. In today’s digital world the purpose behind scytale has evolved and been adapted to modern technologies, including computer software and hardware, and can achieve the same goals scytale was meant to achieve. Not only that, but computer hardware and software encoding, encryption, and password protection has evolved from physical device data storage and protection into digital data transmission, encryption, and protection.

The internet was essential to the increased usage of password protection and encryption. Password protection and encryption allow the internet to be a functional tool for the modern international economy. The internet is a digital transmission system that transfers digital signals across airwaves, satellite signals, and hard-wired brick-and-mortar buildings. Everything that is transmitted in a digital network infrastructure, like the internet, digital television, digital radio, satellite signal, or cell-phone network or communications network system, is encoded, transmitted, received, and decoded in a binary digital format. The binary digital format, wherein everything sent or received must be translated into a system of 0’s and 1’s, and the digital data encryption techniques that accompany the binary system have made encryption and password protection the most desired forms of digital privacy protection.

An Explanation of the Difference between Binary System Encoding and Encryption

The binary system is a fully defined, working, known system wherein it can be readily translated and understood much like any known and defined spoken language used in the world today. A casual look at the binary system might lead one to mistake it for encryption, but this is not the case. The binary system is the language utilized to effectively transfer digital information. The binary system protects data integrity using binary check-sum, which can detect

changes in binary data transmitted from one point to another. The binary check-sum does not secure digital data transmission. In fact, if security was not an essential component of personal and financial privacy encryption would be unnecessary. However, because personal and financial privacy is such an essential component of today’s world and financial structure, data encryption is essential.

Today’s data encryption techniques exist as initially envisioned – unreadable without the originator’s input. Encryption techniques have developed and become more intricate through the utilization of mathematical scales and increased understanding of complex arithmetic. Modern mathematical techniques make decryption much more costly than beneficial in most instances, and temporally impossible in others. As encryption and data protection started to be used in the internet, by the modern military, required by legislative enactments, and mandated by federal entity standard setting agencies the cost of encryption started to go down. As exhibited with Seagate’s hard drive costs, the cost to protect one’s own personal data has reached a point where even a private citizen can afford to encrypt and password protect his or her data.

The Role of Law in Increasing Password Protection and Data Encryption

Federal laws have mandated encryption methods for protection in varying contexts. For instance, transmission encryption is required for certain types of data transmission, and storage encryption methods for everyday data storage have been mandated by other legislation. With regard to data transmission, the Secure Socket Layer (SSL)-128/256 is the encryption technique utilized in data transmission and over the internet. SSL-128 utilizes a method that allows

---

10 Including the National Institute of Standards and Technology (NIST), the Federal Trade Commission, and the Federal Accounting Standards Advisory Board (FASAB), etc.
connected devices to “negotiate a ciphersuite (combination of encryption, randomly created key
and key exchange, authentication algorithms, symmetric or asymmetric, RSA, AES, etc.),” transmit data securely between the negotiated devices, and then destroy the key that was used to
allow the secure communication to take place. Encryption using an SSL-128-bit key certificate
means that the encryption/decryption key being used is 128 bits long.\textsuperscript{12}

In mathematical terms a 128-bit key means there are $2^{128}$ possible combinations for
the 128-bit randomly created security key. The 256-bit key is the strongest current level of
encryption protection\textsuperscript{14} in modern day usage, and this means there are $2^{256}$ possible
combinations. The key limiting factor to selecting 128-bit versus 256-bit encryption protection
is the limit of data transmission speed and delay. Seagate’s BlackArmor user guide explains 128-
bit encryption is the industry standard, and that “[t]he longer the key, the more secure your data.
However, the 192 and 256-bit long keys significantly slow down [transfer].”\textsuperscript{16} Finally, what is
essential about modern day encryption techniques is that for a computer system to break a 128-
bit key encryption, it would take a computing cluster that would envelop the entire earth to a
height of one meter, and then still require 1,000 years on average to recover.\textsuperscript{17} Hard drives use

\textsuperscript{12} Bits are 0’s or 1’s arranged in 8 block increments to a point there is a total of 128 0’s and 1’s linked together. 128-bit encryption is also known as 16-byte encryption. One byte would look like the following: 00000001. 16 blocks of these 8 bit bytes would be chained together to achieve 128-bit encryption. ROB WILLIAMS, COMPUTER SYSTEMS ARCHITECTURE – A NETWORKING APPROACH 24 (2nd Ed. 2006).
\textsuperscript{13} $2^{128}$ EQUALS 3.4*10 raised to the exponent of 38, or 340,282,366,920,938,463,463,374,607,431,768,211,456.
\textsuperscript{15} $2^{256}$ EQUALS 1.157920892 * 10 raised to the exponent 77.
encryption techniques similar to SSL-128/256, just specially adapted for storage within a digital hardware device and the transmission occurs only between the hard drive and the computer processor and then displayed on the computer’s display device.

**The Two Umbrella Encryption Methodologies – Symmetric and Asymmetric**

There are two fundamentally different types of encryption: symmetric and asymmetric. In terms of encryption techniques, symmetric and asymmetric methods are differentiated by the type of key that is generated to access the encrypted data, as well as who has access to the associated key. Symmetric encryption methodologies utilize only one key for both encryption and decryption.

**An Example of Symmetric Encryption**

Digital storage devices can utilize Advanced Encryption Standard (AES) cryptography. AES is a symmetric key system adopted by the National Institute of Standards and Technology (NIST) for encryption of all federal agency or department cryptographic devices protecting classified information. The U.S. Government also utilizes AES for encrypting top secret information. Private Citizens can also access and use the AES encryption standard relatively easily. In addition, with its adoption as the federal government standard, NIST also encouraged non-Federal Governmental organizations to utilize AES encryption when they provide security for commercial or private organizations.\(^{18}\) With regard to an estate being fully executed, this sort of encryption is virtually impossible to break without the given key (assuming the key is not easily guessed or decoded utilizing a key word list.

Similar to SSL-128 bit key encryption for data transmission, AES uses an algorithm to encrypt and decrypt information stored utilizing a 128-bit key. A major concern of all

---

encryption techniques is the overhead that the method will add to the actual meaningful data. AES is efficient in that the 128-bit fixed length block sizes it utilizes when storing digitized information on storage devices is based on a design principle known as a substitution-permutation network\(^\text{19}\) (linked mathematical block-cipher algorithms), which allows the storage and retrieval of AES-encrypted data relatively quickly. The flaw with AES encryption is that the key is required for decryption and the key must be either sent to or held by the person seeking to decrypt it. Box.com’s cloud storage (see below) encryption process uses the symmetric AES encryption for storage and 256-bit SSL encryption for transmission as is exhibited on their web page diagram:\(^\text{20}\)


As is exhibited in the Box.com model, when a consumer utilizes Box.com’s technology, it takes the consumer’s data and stores it in a cloud storage environment. The user of Box.com’s services opens an account, and then has access to AES encryption methodologies on both the user end, the transmission layer (SSL-256 bit), and on Box.com’s cloud infrastructure. As has been discussed, not only is the consumer’s data encrypted when it is at rest, but then it is also encrypted when it is transmitted across the internet’s Secure Socket Layer (SSL). One of the flaws of Box.com’s model is that it uses a symmetric system, so the company itself holds the encryption key – and as such can theoretically access a user’s content at any point in time.

An Example of Asymmetric Encryption

RSA cryptography, the Diffie-Hellman algorithm (RSA), or Public Key Cryptography is an asymmetric method of strong encryption that does not require the transportation and exchange of a key. Rather than having one key that must be transported between the two parties communicating, RSA utilizes two keys for encrypting and deciphering messages. One of the keys in RSA is public and can be known by anyone, and then there is a second key that is only known by the party that will receive the messages. The final recipient (also the creator of the public key) in this encryption system creates two very large numbers, keeps them private, and then before sending his message he multiplies them together giving an even larger number which is the public key. Anyone that wants to send a message to the final recipient then uses the one very large number to encrypt the message. When the final recipient receives the message he or she will be able to decrypt it using the prime numbers used to create the larger publicly known encryption key. With asymmetric encryption, once a message is encrypted, not even the sender can decrypt the message once it is encrypted (only the final recipient/holder of the two prime
numbers will be able to decrypt the message). Here again, if the Responsible Party does not have access to the two private numbers, then they will not be able to decrypt the encrypted data.

**The Password Protected Digital Device**

When a Responsible Party encounters a digital device\(^2\) he or she cannot just begin to access, delete, distribute, copy, or publish data and information held digitally. There are numerous regulations, restrictions, prohibitions, and specific steps the Responsible Party must take depending on the digital data. A good starting point for a Responsible Party encountering digital data is to pose a set of questions to himself, which include:

- Is there potentially government-owned or regulated data on the computer which might prevent me from having authorized access?
- Is there any federal or state law that would protect the digital data held within this digital device?
- Is there any data that may have a security clearance and/or belong to another entity (especially a governmental entity)?
- Is there any law that might prevent me from gaining access to this digital device?
- Is there any data on this computer for which I might per se violate a legal regulation by accessing it?
- Is it legal for me to ‘hack’ or have someone ‘hack’ into this digital device?
- Is there a way that I can figure out what the password to this computer is (or bypass any password in the alternative)?\(^3\)

**Where Initial Question Answers Lead the Responsible Party**

If a Responsible Party attempts to gain or gains access to a digital device that is solely owned by the deceased or incapacitated person, no laws will be violated by circumventing, guessing, or otherwise getting through the digital device’s *initial* password protection – as long

---

\(^2\) In the context of this paper, ‘Digital storage devices’ can include mobile devices, devices that exist in a cloud service, stationary or mobile computer units, and stand-alone devices that provide their own means of access, or those devices that must utilize another digital device for data retrieval.
as the Responsible Party has no reason to believe regulated data is held behind the password protection. If a Responsible Party attempts to access the deceased or incapacitated person’s data, which is hosted by a third party entity, there will be laws that limit, prohibit, and possibly make illegal the Responsible Party’s attempt to access the stored data. If a Responsible Party attempts to access data on the deceased or incapacitated person’s digital device, and the data has been further protected beyond the initial digital device password, the Responsible Party may have limits and prohibitions on circumventing data protections. A Responsible Party may also open himself up to liability for accessing certain data, circumventing protection measures on data, altering the data, destroying the data, or failing to turn illegal material over to appropriate authorities.

**The Computer Fraud and Abuse Act (CFAA)**

The Computer Fraud and Abuse Act (CFAA), 18 USC §1030 makes unauthorized access to a “protected computer” a crime punishable by fine and or jail, states,

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, …

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (m) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

22 18 USC §1030(a)-(j).
23 Id.
(3) intentionally, without authorization to access any nonpublic computer of a
department or agency of the United States, accesses such a computer of that
department or agency that is exclusively for the use of the Government of the
United States or, in the case of a computer not exclusively for such use, is used by
or for the Government of the United States and such conduct affects that use by or
for the Government of the United States;
...
(5)
  (A) knowingly causes the transmission of a program, information, code, or
command, and as a result of such conduct, intentionally causes damage
without authorization, to a protected computer;
  (B) intentionally accesses a protected computer without authorization, and as
a result of such conduct, recklessly causes damage; or
  (C) intentionally accesses a protected computer without authorization, and as
a result of such conduct, causes damage and loss.^[2]^ 

The CFAA provides no exception for a Responsible Party to legally access a computer protected
by it so a problem arises when the data is password protected or encrypted, and the person
accessing it does not know what they are accessing until the information is revealed. For
example, safe-harbor provisions do not exist in legislative enactments covering child
pornography, so it is essential that a Responsible Party can appropriately act if it is encountered.
In addition, federal legislation is not the only concern for a Responsible Party.

States also have “Computer Hacking and Unauthorized Access Laws.”^[24^ Each state’s law
is listed on the national Conference of State Legislatures webpage, which states:

Hacking is breaking into computer systems, frequently with intentions to alter or
modify existing settings. Sometimes malicious in nature, these break-ins may
cause damage or disruption to computer systems or networks. People with
malevolent intent are often referred to as "crackers"--as in "cracking" into
computers.

"Unauthorized access" entails approaching, trespassing within, communicating
with, storing data in, retrieving data from, or otherwise intercepting and changing

computer resources without consent. These laws relate to either or both, or any other actions that interfere with computers, systems, programs or networks.

The appropriate state laws must be considered before any person attempts to gain access to password protected or encrypted data.

**Solutions to Accessing a Password Protected Computer**

Once a Responsible Party has determined that they are able to access a password protected computer – and are fully aware of what they should do if any particular type of digital data is encountered – a computer using a Microsoft based operating system could be accessed in the following manner:

1. An attempt can be made to access the computer using a known or named password list from the incapacitated or deceased.

2. The Responsible Party can obtain software that enables him to reset Windows-based passwords using a software utility tool. These types of software allow a user to reset existing passwords so the computer can be accessed without knowing the password.

3. An attempt can be made to login to the computer by pressing “F8” when the computer boot process starts. Once the “F8” boot option screen comes up, the Responsible Party can select “Start in Safe Mode.” When the login screen comes up, the Responsible can either input “Administrator” into the user field, or select “Administrator” from the drop down user list. If the computer boots up in “safe mode,” this means the “Administrator” user was active without any password being set. The Responsible Party can then reset any “User Account” password by accessing the “User Account” window from the “Control Panel” window, which can be accessed by clicking the “Start” button.

4. The more advanced Responsible Party can attempt to insert the Operating System Recovery Disc and locate the SAM file. If the SAM file is in ISO format, which must be burned to a disc and the computer rebooted with the newly burned disc in the CD-ROM. Once the computer reboots with the newly burned disc in the CD-ROM, he must press “F2” and change the boot menu options so that the CD-ROM is the first accessed drive on the computer. A video complete with instructions for performing this type of password-bypass is available on youtube and various other websites.

---

Finally, if the Responsible Party is still unable to access the “Desktop” of the computer, the Responsible Party should hire the appropriate computer expert to assist him.

**Types of Data Possible on the Computer (Including Assets and Directions to Assets)**

**Encrypted Files**

Once access to the digital device is gained, the files themselves can be encrypted. Some operating system software\(^{27}\) provides a method to encrypt files. Once the files are encrypted, they can only be unencrypted with the encrypting passcode (See Encryption above). In other words, if a Responsible Party removes digital device password protection that does not mean that they have decrypted the files that are encrypted (therefore the Responsible Party may still not have access to encrypted files). Third party software can also be used to encrypt files and data structures. There are no known methods to decrypt data that have been encrypted using SSL-128, AES 128/256/192, or RSA security. Subject to laws and regulations discussed herein, the only ways for a Responsible Party to possibly decrypt files is without having the encoding key is to attempt to hard hack or guess the encryption key (which is beyond the scope of this paper).

**Financial Data Covered by the Gramm-Leach-Bliley (GLB) Act**

A private citizen might own a business that can be defined as a financial institution. The Gramm-Leach-Bliley (GLB) Act defines a “financial institution” as a business that is any business, of any size, that is “significantly engaged” in providing financial products or services, including check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, courier services, and credit reporting agencies\(^{28}\). Because this definition applies to a business of any size, including a sole proprietorship, closely held corporation, or individual as sole shareholder, an executor/ix may

---

\(^{27}\) For example, Windows 8 or Apple’s OS X.

find that they must access, disseminate, destroy, value, and/or potentially sell GLB governed data.

The reason a Responsible Party may encounter encrypted GLB-covered data is because companies defined as “financial institutions” must ensure the security and confidentiality of personal information collected from customers, including addresses, names, account numbers, income and credit histories, and Social Security Numbers\(^\text{29}\) (as required by Federal Trade Commission (FTC) issued safeguards\(^\text{30}\)), and therefore the executor might find the GLB data encrypted or password protected data. The Responsible Party encountering GLB-covered data must also be aware of the Stored Communications Act (below), as well as the FTC’s Safeguards Rule\(^\text{31}\) encryption techniques, password guessing techniques, and what constitutes exceeding one’s authority under the appropriate governing law(s) where no governing exception exists.

There is no doubt that financial entity data security requires digital data encryption in transmission, as well as encryption and password protection for both internet-linked and physical data storage protection,\(^\text{32}\) (whereas physical data storage is that storage on computers that are not networked for reasons of being more securely protected\(^\text{33}\)) so at the very least the Responsible Party must be knowledgeable when accessing unopened, sent, received, or possible stored emails and email attachments when making their efforts to retrieve potentially protected data.


**HIPAA Covered Data**

A Responsible Party may encounter digital data or information that comes under HIPAA privacy protections. The HIPAA Privacy Rule provides federal protections for personal health information held by covered. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. Covered Entities can be doctors, psychologists, chiropractors, and health care information clearinghouses (See Are You a Covered Entity?[^34]), all of which could reasonably invite a private individual to have HIPAA covered data at home on his or her digital devices. If a Responsible Party does encounter HIPAA covered data, he or she must ensure HIPAA is complied with. A complete guide for security rule guidance and compliance can be found at the Health and Human Services webpage.[^35]

**Unencrypted Files**

Once a password protected digital device is accessed, the Responsible Party should systematically open and view unencrypted files. As files are accessed, an inventory should be developed. Computer files are very useful to help find information about a person’s monthly bills, assets, account locations, beneficiaries, liabilities and asset locations.

**Intellectual Property**

A digital device can hold extremely highly valued intellectual property and information. Intellectual Property contained on a computer might include copyrighted or copyrightable


material, digital assets that have been purchased from a 3rd party, trade secrets, patents and patents pending, and trademark development or trademark information. In addition, a digital device can also hold data that has no monetary value, but is priceless to a deceased party’s loved ones. There are immeasurable amounts of data and information that can be held on the digital devices of today.

**Spreadsheet and Accounting Files**

A Responsible Party may encounter spreadsheets on digital devices. A spreadsheet of assets, liabilities, or monthly bills can help paint a picture for a Responsible Party. In viewing a spreadsheet, a Responsible Party can start to know what they need to address, where they can start to distribute an estate, or how to carry forward a person’s life. Some computers may also hold accounting software and user files that hold even more detailed information about a deceased or incapacitated person’s bank accounts, credit cards, or other valuable Id’s, keys, or locations.

**Adult or Child Pornography**

If the Responsible Party comes across pornographic material, he should immediately seek to discover if the deceased or incapacitated is harboring illegal illicit material such as child pornography. Child pornography is defined by 18 U.S.C. §2256, and criminalized and penalized under 18 U.S.C. §1466A, and the set of laws make holding such material a strict liability crime in that merely holding such material is criminal. Every state in the United States has similarly passed strict liability laws reinforcing the federal statutes. A Responsible Party must understand exactly what type of pornographic material is stored on a computer because the pornographic videos, pictures, scripts, web site products, etc. contained on a digital device could

---

be assets to a business if they are not child pornography. This is further incentive for a Responsible Party to get to know who their client is or was, and what type of businesses they could be involved in.

**Computer History, Registry, and Temporary Files**

A Responsible Party should look at browsing histories, temporary computer folders and files, and the computer registry. Computer history files and registry entries can reveal web pages that the deceased or incapacitated visited, and this can lead to web pages that provide access to accounts listed in Office spreadsheets, and lead to email and social media sites holding links to friends, relatives, and associates.

**Internet Content**

A computer can direct a Responsible Party to online portals, which include login pages for any type of internet accessible account. A Responsible Party may be able to determine which online portals a person uses with a simple analysis of the temporary internet files or web browser history. However, because a user may delete his or her browser and history files, an analysis of the temporary internet files or web browser history may not lead to all pertinent information. Therefore, a Responsible Party must also analyze the ‘computer registry.’

A computer registry is nothing more than stored computer configuration settings, but this structure can have a massive impact on one’s computer system. Because of the computer registry’s ability to quietly work behind the scenes of a computer’s operation, the computer registry can be used to insert hidden virus software, 37 access a computer remotely, and even set

---

the computer to remotely run automatic processes and updates. Microsoft warns the computer user, “[s]erious problems might occur if you modify the registry incorrectly.” These types of warnings often deter even more advanced uneducated computer users from deleting items from or even accessing the registry, so it remains a potential valuable source of information.

Instructions for gaining access to the registry can be found in footnote 29.

Access Limitations on Web Portals the Responsible Party Was Directed To

Once a Responsible Party makes a list of all of the web sites visited and software utilized by a deceased or incapacitated person, he or she must be aware of the Terms of Service (ToS) and federal laws that can make access to data, assets, and information stored in digital devices prohibited or illegal.

Terms of Service (ToS)

The Terms of Service (ToS) is a contract between a web service provider and the user that describes what a user can and cannot do when operating on the service provider’s web page when logged into a created account. The Responsible Party must be aware of what they can and cannot do in order to obtain access to each individual online account before taking any action.

An example of the variability of ToS contracts, Yahoo! and Twitter’s transferability and survivability ToS provision differences follow. Yahoo!’s ToS state:

---


You agree that, except as otherwise expressly provided in this TOS, there shall be no third-party beneficiaries to this agreement. … 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.41

On the other hand, while Twitter’s ToS42 do not specifically address transferability of an account, the ToS do state the user retains the rights to content posted, and that Twitter can “…suspend or terminate your accounts or cease providing you with all or part of the Services at any time for any reason…”43 Because a deceased or incapacitated person could hold assets and valuable information in online accounts, in order to properly obtain, retain, and distribute the deceased or incapacitated person’s estate and assets the Responsible Party must be aware of ToS limitations.

The Stored Communications Act

The Stored Communications Act (SCA – 18 U.S.C. Chapter 121 §§2701-2712) is law that addresses disclosure of data held online by third-party internet service providers and account services. The SCA criminalizes intentional access to facilities wherein the access intentionally exceeds authorization. Orin S. Kerr explains the SCA as a “sound approach to the protection of stored Internet communications,”44 by stating that the protections were necessary because the Fourth Amendment’s scope of protection did not include internet communications (which inherently disclose data and information to third parties. As such, when the Responsible Party

43 Id.
seeks to access email accounts, online bank accounts, and online investment or trading accounts, social media accounts, or any other account that exists online, he or she will inevitably contend with third party invocation of the SCA.

**An Example of How the SCA Can Be Used to Prohibit Access**

On September 20, 2012, the United States District Court for the Northern District of California granted Facebook a motion to quash a subpoena requiring it to turn over the contents of a member’s facebook.com account in a civil lawsuit moving to dispute whether or not the member committed suicide. The court’s reason to grant Facebook.com’s motion to quash the subpoena was because “[t]o rule otherwise would run afoul of the “specific [privacy] interests that the Stored Communications Act (SCA), 18 U.S.C. §2701, et seq, seeks to protect.”

In addition to the court’s ruling citing the SCA, under the Facebook’s ToS states, “You will not solicit login information or access an account belonging to someone else” The court basically agreed with Facebook when it blocked access to third parties without a subpoena. It used the SCA to do so. Therefore, it seems inevitable that the only way to mandate a company must turn over information held behind its online portal is with court validation of appropriately drafted Responsible Party-friendly state legislation (which is a discussion for another day).

**An Example of How the SCA can Provide Protections**

The SCA makes a distinction between communications held in electronic communications services, which require a search warrant and probable cause, and those in remote computing services, which require only a subpoena or court order, with prior notice. For instance, on July 8, 2011, in CCA 2011-41-017, the IRS sought out to obtain a taxpayer’s e-mail

---

45 United States District Court. Northern District of California. San Jose Division. Case No.: C 12-80171 LHK (PSG). Order Granting Facebook, Inc.’s Motion to Quash.
46 Theofel v. Farley-Jones, 359 F.3d 1066, 1074 (9th Cir. 2004).
contents and non-content information from the taxpayer’s Internet Service Provider (ISP),
without a warrant. Chief Counsel concluded that the IRS could obtain non-content information
under §2703(c)(2) of the SCA, but could not obtain the taxpayer’s ISP email contents because it
would violate SCA §2703(a), which requires a non-governmental entity to obtain a warrant to
compel disclosure of electronic communications in electronic storage for 180 days or less. The
IRS case is an example of protections that the SCA provides.

Cloud Computing

The SCA is becoming even more applicable to estates as cloud computing becomes more
prolific. Some companies utilize Cloud services to store email account, social media accounts,
etc.; for those companies the ToS will be the end user agreement. Where companies are using
Cloud software administration or Cloud storage for their storage network, they do so because of
its cost-effectiveness, scalability, and hardware resource efficiency, and because of excess
storage capacity from company usage, cloud computing has become cost effective for the
individual. For individuals that use Cloud services, they can purchase the usage of software and scalable storage on a percent used and amount of storage needed, basis; the agreement that
governs access to the cloud by a Responsible Party will also be governed by the Cloud Service
Provider’s ToS and the SCA.

Conclusion

In conclusion, a digital device can hold vast amounts of financially valuable and
hereditarily invaluable information. Because the world is becoming more technologically savvy,

---

48 James D. Lamm, Digital Death: Estate Planning for Passwords, Online Accounts, and Digital Property,
Presented at: Gray Plant Mooty; Saint Cloud, MN, 7/26/2012.
service-type-cloud-services.
50 Top-10-Online-Backups.com., Top 10 Cloud Storage Providers Reviewed, Nov. 2, 2012,
not only have governments integrated encryption and password data protections and mandates, but individuals have gained a more cost-effective and easily utilized way to protect data that they do not want seen by anyone else. A problem arises when an individual either dies or becomes incapacitated to a point where they are unable to tell others how to access their password protected or encrypted data. Not only does a person’s estate decrease in worth to others when this happens, but if the incapacitated person is able to recover then they will have a mess to deal with when they are finally able to get their affairs in order on their own. This paper is intended to educate the reader about current technology, as well as make him or her aware of types of data, legislation covering it, what to do when a digital device is encountered, and how to most fully recover assets and carry forth an incapacitated person’s life. Without the considerations herein, a Responsible Party will surely fail at being as effective as possible.