ASA

Risk Consultants

Research Note

Risks in Digital Identity After Death

By: Jess Mauer

Keywords: Death, Identity, Risk, Privacy

Abstract – People have been transitioning remnants of their identity from conventional physical effects, such as photos and trinkets, to online profiles and social networks. Identity is being digitalized and with this, complications arise as the population ages. A death today presents more complex issues than before the digital age. The component of an online identity does not fit in the mold of our society's traditional framework for dealing with death. This research note explores the new risks regarding the ethics, legality and privacy of an individual's digital identity after their death.

ASA

Risk Consultants

Introduction

People have been grappling with digital identity issues since objects have expanded into digital space, rather than just the physical world. People crossed a threshold some time ago, where it became easier to create things online rather than to purge them. The results are overflowing inboxes, camera rolls and status updates. Now that we can store thousands of photos on our smart phones and with Facebook reporting a billion active users last year,[1] there's no need to be discerning when deciding what objects of your past to keep; you can keep everything, and keep it online — a concept that the general public has accepted with such relish that seeing a photo album in someone's home almost feels quaint.

Amassed over a lifetime, these digital photos, emails and status updates paint a story of someone's identity in a way that a shoebox of trinkets used to. However, identity is different when it's digital. Physical remnants don't have controls provided to online accounts and can be contained in one location. Also, because they are physical things, they have to be purged. An individual must make concerted decisions about what to keep and what to get rid of. On the Internet, these "trinkets"

could be strewn among a multitude of different sites, amassed in huge quantities.

As this data is collected and cultivated in an online space, it develops into a user's identity, access to which is locked behind a password. This becomes a complicated problem when the user passes away. After a loved one dies, a troubling but natural process for survivors is to go through the decedent's remaining possessions for memorial and closure. This process becomes drastically altered if everything is password protected and inaccessible.

A simple solution might be disclose your password to a trusted source in the event of your death, which begins a slippery risk slope of gray areas. First, facing one's own mortality is a commonly avoided topic. Most Americans don't even have a will, so it's no surprise that planning for what would happen to their digital identity after death is not on most individuals' radar (a quick Internet search found from 30 to 50 percent are will-less, but I couldn't find a specific verifiable source on this). If someone were to pass away unexpectedly, a surprisingly lot more is lost to their loved ones if they do not know the passwords or do not even know where to look online.

Those who are attempting to develop an appropriate framework for this problem are floating ideas like having an "authorized user" attached to social network accounts or sharing their passwords with a trusted source.[2] However the legality of this is unclear, as will be discussed later in this research note. Moreover, not every user is willing to have this kind of disclosure. The uneasiness of thinking about death combined with the uneasiness of sharing access to a "private" space makes it easy to see why people don't want to deal with this emerging problem.

Just like anything else that people typically do not enjoy doing, there are options to pay someone to provide a solution to maintaining your digital identities securely for your beneficiaries. A few of the main options are sites like Legacy Locker and Asset Lock. Both sites allow you to assign a beneficiary and recommend you use their space as a one-stop digital backup for all your valuable documents (deeds, trusts, etc). Thankfully, both sites claim to use 256 bit encryption and SSL. Privacy is another issue. While Legacy Locker states explicitly they will not share user data with 3rd parties for marketing, Asset Lock does disclose that they aggregate user data to 3rd parties — which shouldn't exactly instill comfort in those thinking about linking all their banking, email and

social media. Asset Lock does address a risk of future uncertainty in their business by having a policy if they are shut down.[3] A user wouldn't be able to locate an equivalent policy with Legacy Locker.[4]

Then there are sites like Death Switch, which allows users to upload messages to send to specific individuals upon their death. The site recommends using the message service for banking information, funeral plans, computer passwords, love notes or unspeakable secrets. The user is emailed periodically to verify that they are still living and if an answer is not received, the messages are sent.[5] This seems like a great premise for a summer blockbuster considering the amount of emails that get lost in my inbox.

Risks

While the startups are figuring a way to profit from this digital identity after death, it's important from the risk assessment perspective to take a closer look at the gray areas involved in these decisions.

Risk #1 - putting all your digital/personal identity in one location creates a single point of failure and a huge risk to your data privacy, especially considering the type of information they recommend you upload to their servers. Sites like Legacy Locker or Asset Lock could have a breach. They could fail as a business and shut down. Or with no

transparency in this space, they could lie about what they are using your data for. These businesses haven't been around long enough to gain user trust. Storing your data over a lifetime is a long time when the average online startups fail 30 to 40 percent of the time.[6] This risk is high for the user — having this data lost or compromised would be detrimental on their online identity.

Risk #2 - it's probably illegal. It's definitely against the terms of service of many of the popular social and electronic communication sites. Whether someone might disclose login information to one of the digital afterlife businesses or to a significant other, they are still disclosing something they agree not to do when signing up for these sites. Here are a few examples:

Facebook	"You will not share your password, let anyone else access your account, or do anything else that might jeopardize the security of your account."[7]
Yahoo	"You are responsible for maintaining the confidentiality of the password and account and are fully responsible for all activities that occur under your password or account."[8]

LinkedIn	"You agree to: 1) keep your password secure and confidential; 2) not permitted to others to use your account; 3) not use other's accounts..."[9]

Legally speaking there is not much precedent to follow; however it is technically against the law, at least according to the Computer Fraud and Abuse Act. This act makes any unauthorized access of an online account a criminal offense.[10] This is also true based on the Stored Communications Act, which was originally created to enhance the rights of privacy extended by the 4th amendment to the digital realm.[11] This is a good thing, but when it's utilized in the context of a user's death, it can be used to bring criminal penalties for unauthorized access of electronic communications and remote computing services. Criminal penalties that could arise from disclosure of your password and login information as the businesses mentioned above require for their business model to function, making it risky to the users and their executors or to the businesses running digital afterlife planning sites.

A lot of social media sites understand this, which helps to mitigate the risk. Facebook has gone so far as to create an option to put someone's timeline in a "memorial" state, where users can still post

messages, photos and videos. But no one can log on, only confirmed friends can see the content, and private messages remain private. This is an interesting compromise because it allows those grieving to have a space to come together and share memories and feelings in a way that is very organic to our current generation. However, it does have its limitations. The page of the deceased is locked down in order to prohibit new friends from being confirmed and the private messages from being read.[12]

Sites that don't have a service like this, like a blogging site, remain accessible in their current state, but run into another familiar Internet problem — spambots. Nothing could be more disrespectful to someone's memory than to have their blog filled with spambots with no way to remove them if site login is not possible.

On the other hand, allowing anyone, even an estate executor, to log into any of the decease's online profiles violates the essence of an access controlled space. Which brings up ethical implications regarding how our society should handle the privacy rights of the deceased.

Risk #3 - The privacy violations of the deceased user. Would users be willing to use these sites for their intended purposes if they know this information would be released upon their death? What happens if,

upon death, a user's privacy is violated by someone who gained access to their online accounts and defamed the deceased's character? Social media sites also need to protect the integrity and authenticity of their product and protect user trust. Any violation of privacy, even to a deceased user, reflects negatively on their business and brand integrity.

States are slowly beginning to create legislation to support people going through this process. Five states have laws on the books for digital estate planning and many more have laws in the works. Connecticut was the first in October 2005 with Public Act No. 05-136. This requires email providers to provide estate executor with a copy of deceased individual's mailbox contents. Other states followed; Rhode Island in May 2007 with HB 5647 and Indiana in July 2007 with Code 29-1-13. It wasn't until Oklahoma passed HB2800 in November 2010 that there was any verbiage explicitly stating social networking or the ability to do more than just have a downloaded copy of the content. HB2800 stated that executors had the right to control, continue or terminate any online accounts of the deceased. Idaho passed a similar law in July 2011 and many more states plan on following.[13]

Conclusion

Response to all three of these risks is a matter of acceptance or sharing. Using a third party site to organize digital assets can be seen as a shared response with the site. However the most likely risk response is acceptance. While technically possible that any type of password disclosure or "unauthorized access" could receive criminal penalties, this has yet to occur and it seems like our legal system has bigger fish to fry. In addition, as sites like Facebook have shown their "memorial" profiles and states like Connecticut, Rhode Island, Indiana, Oklahoma and Idaho have put laws on their books, it's clear this is an issue that is getting visibility. The only risk that remains high is one of privacy. It's hard to say how much access will be allowed in the future, but as more and more states pass laws allowing estate executors access to all online accounts to continue, maintain or terminate them, a pattern is developing. A pattern that doesn't take into account a method to understand a user's last wishes or who may access their online information after they pass. In death, as in life, there is always a counter balance of privacy and security access. Who has access to your shoebox of trinkets or a safety deposit box is a very personal decision, and the same applies to anything online. It will be interesting to see

where on the spectrum the future standard of digital access after death lands.

ASA

Risk Consultants

References

[1] Crawford, D. (2013, January 30). Facebook Reports Fourth Quarter and Full Year 2012 Results. Facebook, Inc.

[2] Walker, R. (2011, January 5). Cyberspace When You're Dead. The New York Times. Retrieved from http://www.nytimes.com/2011/01/09/magazine/09Immortality-t.html

[3] Asset Lock. (2012). Retrieved from http://www.assetlock.net/terms/

[4] Legacy Locker. (2009, March 18). Retrieved from http://legacylocker.com/support/terms-of-service

[5] Death Switch. (2006). Retrieved from http://www.deathswitch.com/terms.html

[6] Gage, D. (2012, September 19). The Venture Capital Secret: 3 Out of 4 Start-Ups Fail. Wall Street Journal. Retrieved from http://online.wsj.com/article/SB10000872396390443720204578004980476429190.html

[7] Facebook. (2012, December 11). Retrieved from https://www.facebook.com/legal/terms

[8] Yahoo. (2012, March 16). Retrieved from http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html

[9] LinkedIn. (2013, May 13). Retrieved from http://www.linkedin.com/legal/user-agreement

[10] Eltringham, S. (n.d.). Prosecuting Computer Crimes. Office of Legal Education Executive Office for United States Attorneys. Retrieved from http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

[11] Kerr, O. S. (2004). A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It (SSRN Scholarly Paper No. ID 421860). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=421860

[12] Facebook, n.pag.

[13] Carroll, E., Carter, J. G., Greenwood, D., & Romano, J. (n.d.). Law. Digital Estate Resource. Retrieved June 8, 2013, from http://www.digitalestateresource.com/law/