

Keeping Your Digital Legacy Safe

Heather Moorefield-Lang and Jeffry Lang*

When working with technology, it is important to be safe and secure online, but what happens to your digital legacy when you are no longer here? In other words, does the internet know you're dead? How can your family, friends, or loved ones gain access to your digital files, social media, and other portions of your online life? Inheritance laws have dealt only with physical property until the last few years. There is little regulation in place for online items (Zastrow 2017). We have built so much of our life online. We must think of that digital life we leave behind. Do your heirs know how to access your cloud-based files? Can your social media sites be shut down? What do you own online versus what access rights do you have to view, listen, and read online? At the simplest level, can your family access your laptop, computer, tablet, or phone? We work so hard to be safe digital citizens online that we forget to think about a time when we are citizens no more.

Useful Terms

The following items can be incredibly useful for family, friends, and loved ones needing to access your digital belongings:

- *Death certificates.* A death certificate is an official document, signed by a physician, that provides the cause, date, and place of the person's death. When a loved one dies, death certificates are needed for a variety of things, everything from insurance to banking. Death certificates are often needed for social media and cloud accounts.

Facebook, Twitter, Pinterest, and others request a death certificate to close an account (Lexikin 2019).

- *2FA.* Two-factor authentication (2FA) is considered an extra layer of security for account access. Typically, e-mail will have a username and password. Using 2FA means another piece of information is needed for access. This extra piece of information might be a secret question, a PIN, or a code sent to your phone or device, or it can be biometric such as fingerprint, iris, or voice (Authy 2020). Two-factor authentication is useful for digital security but can be bad when someone passes away, especially biometric 2FA. This is another reason why communication is important among family members and having a family password manager is useful. Read about password managers in the next paragraph.
- *Family password manager.* Think of a password manager as an online version of a notebook. This is a place to store all account log-ins and keep notes for your heirs (Pinola 2019). These online storehouses let users store passwords and log-in information while also keeping this data secure and private.
- *E-mail accounts.* Many online accounts are tied to e-mail addresses and can often be used to unlock or recover other accounts. It is important to maintain access to these e-mail accounts as many are purged after a certain amount of inactivity.
- *Licensed software, photo, music, and data repositories.* Many of these are subscription-based services that are autobilled to credit cards, and their data retention policies vary. Often, accounts are

* **Jeffry Lang** works as a lead security analyst for the Security Office at Virginia Tech. He has worked in various areas of information technology, including computing technology system administrator and technology manager for multiple organizations. Jeffry has a BA in philosophy from UNC Greensboro and a master of information technology from Virginia Tech. He has experience with network monitoring and forensics, intrusion detection, and configuring security appliances. He is a SANS Certified Intrusion Analyst, Windows Security Administrator, Network Forensics Analyst, Certified Detection Analyst, and Enterprise Defender.

purged after a certain amount of inactivity.

- *Monetized social media, digital pay apps, virtual goods, and cryptocurrency.* Online activity can often lead to real monetary assets or even virtual assets. The IRS recently updated a policy that determines which digital assets are taxable and excluded in-game currency in reporting responsibilities (Phillips Erb 2020).
- *Cryptocurrency.* According to research by the *Financial Times*, between 2.3 million and 3.7 million Bitcoins have been lost for a variety of reasons, including the death of the asset holder, which accounts for roughly 30 percent of the Bitcoin market (Goldring and Jacobs 2019). Cryptocurrency is also a taxable item according to the IRS and subject to inheritance taxes, even if the currency is inaccessible (IRS 2020).

Online Tools You Can Use

- *1Password.* 1Password is a site for your family and you to store and share passwords, software licenses, notes, and other items that might be sensitive.
- *LastPass.* LastPass is all about making your online life easy. This is a spot to share and remember all your passwords across devices. The site works very similarly to 1Password in that you can set up accounts for your family to share passwords, notes, and other sensitive information.
- *Gmail.* Inactive Account Manager from Gmail allows you to plan for what happens when you pass away or when you stop using an account.

1Password
<https://1password.com>

LastPass
<https://www.lastpass.com>

Gmail Inactive Account Manager
<https://myaccount.google.com/inactive>

Final Tips and Considerations

- If you have not already done so, speak with an estate attorney about your physical and digital property. If you don't want to involve a lawyer,

research writing a will online. It is an easy document to fill out, and you need only a notary stamp to make it official.

- Talk with your family, friends, loved ones, and heirs. Death is not the most exciting or welcome of topics, but it happens to 100 percent of us. Not discussing it is leaving your heirs in the lurch.
- Appoint a digital executor. This can be the executor of your will, or it can be a designated web service (Zastrow 2017).
- Be realistic about your digital assets and belongings. What do you have? Make an inventory for those who will inherit. Update this list and revisit regularly (Zastrow 2017).
- If this topic is of interest to you, see our list For Further Reading below for more information.

For Further Reading

- Carroll, Evan. 2017. *10 Simple Steps to Get Your Digital Life in Order: A Guidebook to Help You during This Difficult Time.* Raleigh, NC: Digital Beyond.
- Carroll, Evan, and John Romano. 2010. *Your Digital Afterlife: When Facebook, Flickr and Twitter Are Your Estate, What's Your Legacy?* Berkeley, CA: New Riders.
- Crocker, Angela, and Vicki McLeod. 2019. *Digital Legacy Plan: A Guide to the Personal and Practical Elements of Your Digital Life Before You Die.* North Vancouver, BC: Self-Counsel Press.

References

- Authy. 2020. "What Is Two-Factor Authentication (2FA)?" <https://authy.com/what-is-2fa/>.
- Goldring, Simon, and Elysa Jacobs. 2019. "Cryptocurrency—Current Investment, Future Inheritance." *National Law Review*, May 1, 2019. <https://www.natlawreview.com/article/cryptocurrency-current-investment-future-inheritance>.
- IRS (Internal Revenue Service). 2020. "Virtual Currencies." <https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies>.
- Lexikin. 2019. "How to Close Social Media Accounts When Someone Dies." <https://www.lexikin.com/guide/close-social-media-accounts-when-someone-dies/>.
- Phillips Erb, Kelly. 2020. "After Confusion, IRS Clarifies Tax Treatment of Fortnite and Gaming Currencies." *Forbes*, February 15, 2020. <https://www.forbes.com/sites/kellyphillipserb/2020/02/15/after-confusion-irs-clarifies-tax-treatment-of-fortnite-gaming-currencies/#19ca182c2074>.

Pinola, Melanie. 2019. "Get Your Digital Accounts Ready in Case of Death." *New York Times*, October 3, 2019, updated October 7, 2019. <https://www.nytimes.com/2019/10/03/smarter-living/wirecutter/get-your-digital-accounts-ready-in-case-of-death.html?smid=nytcore-ios-share>.

Zastrow, Jan. 2017. "Online Legacies and Digital Estate Planning." *Computers in Libraries* 37, no. 5: 12–15.