Consumer Reports

What happens to your Facebook profile after you die?

Your online accounts and profiles can live on after you die. Here's how to plan for your digital afterlife

Published: April 21, 2015 04:00 PM

Life used to be so simple. You lived, you died, and the assets you amassed during your time on earth were passed on to your heirs. Now, however, there is some new unfinished business that needs to be taken care of before you go: your personal digital assets.

What are these? Well, your Facebook wall is one of them. The digitized thoughts, photos, and videos that you post there are stored at data centers in the U.S. and Sweden. And think about all of the other Internet services with storage features that you've come to rely on—among them mobile bank accounts, online mutual-fund accounts, and bill-pay accounts.

If you write a blog, you may have years of published material online. If you operate an Etsy account, sell stuff on eBay, or own an online business, you have even more property scattered about on so-called cloud servers. We've all amassed a king's ransom of those personal digital assets. One study released by McAfee, the security technology company, estimated their average value at almost $55,000 in the U.S.

The problem is, "after you die, there's no one monitoring all these assets anymore, which makes them vulnerable to theft," says Gerry W. Beyer, a professor at Texas Tech University School of Law and a leading expert on the estate-planning aspects of digital assets.

Complicating matters, secret usernames, passwords, and other login codes used to keep intruders out die with you. That makes it very difficult or even impossible for your survivors to take proper control of your digital assets. State laws granting rightful access to survivors are in their infancy, while user agreements usually bar access by others to protect their customers' privacy.

Here is Beyer's advice for properly protecting your digital afterlife.

Start with an inventory

Because it's easy to save frequently visited website addresses on your Internet browser's bookmarks bar, the first entry in your paper-based inventory should be a list of the usernames, passwords, and other login access codes to your computers, tablets, smart phones, and other connected devices. Do the same for your encrypted hard drives, flash drives, and other storage devices; encrypted home network routers; voice mail; and any fobs, cards, or other physical digital-key devices that require multifactor authentication security.

Your inventory on paper should then list the Web addresses where your trusted agent can access your account-login pages, along with the necessary e-mail accounts, usernames, passwords, security codes, and login procedures. Don't forget the information needed to reset the password, often your e-mail address where a reset code will be sent, and the secret "Who was your best childhood friend?" question(s), whose answers only you know.

When it comes to estate planning, there's plenty to think about in addition to your digital assets. Check out our Parents' guide to creating a will.

Find and appoint an agent

Because there may be indecorous photos or e-mails or other digital secrets you don't want your survivors to see, take steps to prevent a family National Enquirer eruption. Neatly segregate the indelicate material from the harmless, find and retain a trusted third party to handle your digital affairs, and instruct him on how to manage it. This is best handled by a family attorney, executor, or estate administrator.

Draw up a power of attorney

Don't put instructions and access information into your will because that becomes a public document once it's admitted into probate. Instead, have your estate attorney draw up a digital-assets durable power of attorney. That will legally authorize your attorney or the trusted agent you name to gain access to your accounts and devices, should you become incapacitated, incompetent, or otherwise unable to handle your own affairs. Your agent's authority under the durable power of attorney ends when you die, but thereafter, your personal representative (executor under a will, administrator if intestate) picks up the authority to act.

Store your inventory safely

Of course, all of your access codes are the keys to your digital kingdom, so the printed inventory should be kept securely in a safe-deposit box, Beyer says. Maintain a digital version of your print inventory to note changed passwords or newly added Web services. Store that on an encrypted flash drive, and retrieve and update the paper version as often as is feasible. Destroy the old print list after the new one replaces it.

Look for user controls

Online services have not yet caught up with the digital afterlife concern. "Many have some sort of policy in their user agreement that may allow access to an executor or authorized agent upon submission of a death certificate and documentation," Beyer says. "The industry could solve the problem by providing a screen when you open an account, asking who you authorize to have access if you become disabled or deceased."

But Beyer expects companies to get up to speed on this in the coming years, and some have already done so. Google's Inactive Account Manager, launched in 2013, lets you instruct the Internet giant on what to do if your account becomes inactive for any reason, including your death. You can choose to have your data deleted after three to 12 months of inactivity or authorize trusted contacts who can receive data from some or all of your Google services, including Blogger, Drive, Gmail, and YouTube.