Digging your own digital grave: how should you manage the data you leave behind?

Patrick Scolyer-Gray, *Deakin University*; Arash Shaghaghi, *Deakin University*, and Debi Ashenden, *Deakin University*

Throughout our lifetimes we consume, collate, curate, host and produce a staggering quantity of data – some by our own hand, some by others on our behalf, and some without our knowledge or consent.

Collectively, our “digital footprints” represent who we are and who we *were*. Our digital legacies are immortal and can impact those we leave behind.

Many of us take steps to secure our privacy while we’re alive, but there’s mounting evidence that we should be equally concerned about the privacy and security risks of our “data after death”.

Reincarnation as data

It might be tempting to think of data after death as inconsequential – after all, we’ll no longer be around to worry about it. However, Facebook and Instagram both support static “memorial” accounts for the deceased. We also know memorial pages can play an important part of the grieving process.

Facebook has around 300 million accounts belonging to the deceased. Research suggests this figure could rise into the billions within decades.

However, these platforms’ terms of service don’t address how the data of deceased users is retained, processed or shared.

There is now even more cause for concern with the emergence of platforms like TikTok and Likee, which have both proven to be particularly liable to expose the personal lives of millions online.

This raises important questions, such as:

- what are platforms such as Facebook doing with the data after death they collect?
- is it ever deleted?
- could it be sold or otherwise monetised?
- what assurances do we have our data will continue to be hosted by those providers after death?
- if not, who will be able to access and manage our data in the future?

In 2012, a teenage girl died after being hit by a subway train in Berlin. Her parents had her Facebook credentials and wanted to access her account to determine whether she had committed suicide. After six years of legal battles, the parents were awarded a court order and finally given access to their child’s “memorial” Facebook account data.

We all have skeletons in the closet

COVID-19 has completely changed our internet use patterns. The unplanned transition to working from home has blurred the boundaries between our professional and personal lives.

Consequently, personal information is now more likely to be exchanged over services such as Microsoft Teams. Many users may choose to store confidential information on personal cloud services for the sake of convenience.

With these changes in behaviour, new vulnerabilities have emerged. When a user dies, it’s now more important than ever personal and otherwise sensitive information is automatically identified and secured.

Working remotely or in networked teams can make data less secure.
John Schnobrich/Unsplash, CC BY

Colleagues of the departed may forget to revoke access credentials, which can then be used to steal intellectual property. Embarrassing email exchanges that belonged to the dead can damage reputations, and sensitive information can negatively affect entire businesses and potentially ruin lives.

In 2016, a Twitter account belonging to the well-known US journalist David Carr was hacked by a sexting bot a year after his death. Earlier, in 2010, 16-year-old vlogger Esther Earl died of cancer before she could cancel a tweet she had scheduled for release that left friends and family in shock.

The need for data management after death

Most Australians don’t have a conventional will, so it’s not surprising the digital equivalent hasn’t gained traction.

In collaboration with the Australian Information Security Association (AISA), we surveyed about 200 AISA members to assess their awareness of digital wills and associated Australian regulations that protect users’ security and privacy. Our survey results confirmed that even key decision-makers in the field and cybersecurity thought leaders had not considered or prepared for posthumous data risks.

But raising awareness is only part of the battle. There are no national regulatory bodies, rules or standards for service providers to follow when managing the data of the deceased. And in Australia, there are no laws or regulations imposing requirements to minimise the risks of data after death.

We need a solution that can resolve issues ranging from moral quandaries about posthumous medical data, to privacy concerns about accessing past digital correspondences.

To be effective, such a solution will require legal and policy recommendations, guidelines and technological adaptations for providers, decision-makers and users. Each aspect will need to be sensitive to context and accommodate for grief and mourning among individuals and organisations. For example, there is often a period of compassionate leave available for employees when members of their immediate family pass away.

Some processes meant to manage data after death already exist, but they need more development. Technological solutions for data after death proposed thus far fall into the category known as privacy-enhancing technologies – tools meant to protect users' privacy.

Users have been reluctant and slow to adopt privacy-enhancing technologies. In part, this is because they don't allow individuals the ability to control how they manage their privacy risks.

Patrick Scolyer-Gray, Research Fellow, Cyber Security, *Deakin University*; Arash Shaghaghi, Lecturer, Cybersecurity, *Deakin University*, and Debi Ashenden, Professor of Cyber Security and Human Behaviour, *Deakin University*