

## Mosaics of personal data: Digital privacy during times of change

Professor Wendy Moncur, University of Strathclyde

- Most of us are deeply entangled in digital infrastructures, with fragments of our personal data scattered across multiple platforms and across time by ourselves and others.
- Linking these data fragments can produce a mosaic that affords significant and unintended insights to others – both human and AI.
- HCI, UX, and UxD professionals have an opportunity to develop usable privacy-enhancing tools that nimbly assemble an individual's mosaic of personal data across platforms and across time, and reflect it back to them so that they can understand and curate what they reveal of themselves, and to whom.

### Introduction

All of us go through times of change. Some of these changes can be personally significant and socially sensitive. We should have choices about what details, if any, related to the change are shared with others. Sometimes, we may need to distance ourselves or even sever ties with people we were previously connected to. But privacy can be elusive as digital technologies and the World Wide Web pervade almost all aspects of our lives. While understanding our own needs to balance privacy and connection is hard, navigating available options for sharing is often even harder. Why is the case? Digital technologies and internet services pervade almost all aspects of our lives. Most of us are deeply entangled in digital infrastructures, our data collected, assembled, and at risk of being leaked. Our information can be shared with a much larger audience than intended and much longer than we intended—long after the information may even be relevant - and past ties may be hard to truly sever.

In this article, I'll look at what personal data is, who shares it, and why it is so tricky to control once shared. I'll then give examples of how significant life changes can create greater demands on us around how we navigate and negotiate the privacy, or at least controlled sharing, of our data. I will share some tips around what questions to ask, how to work through scenarios that may or may not work for you, and hopefully help to guide decision-making.

### Personal data

Personal data is "*the digital data that is descriptive of an individual*", the "*...mosaic, persona, ...digitally extended self.*" (Parkinson et al., 2018 ). It involves the person's real name, pseudonyms, and any data linked to that person's identity. It also refers to anonymous content that does not *intentionally* reveal their identity but does so incidentally. Personal data encompasses seemingly mundane information such as name, address, date of birth, photos, social media posts, and location. It can also include sensitive information such as sexuality, sexual preferences, and anything about their current or past sex life; political and religious views; health information, genetic and biometric data, fingerprints, facial recognition; personal interests and affiliations such as trade union membership; cultural and social identity; and financial information such as company directorships, employment, contributions to charities. Such information can potentially be recorded across many platforms and across long periods of time, and thus be available for subsequent retrieval, analysis, and re-posting.

The mosaic of personal data isn't just created and shared by the person themselves; it is co-constructed. Many of us will be tagged in social media posts by friends and family. We will be on voters' registers and perhaps company directorships, held and made visible by Government agencies. Our profiles may appear on our employers' websites. A bystander at a public event may include us in their footage of the event and post it online - inadvertently revealing our location, who we are with, and what we are doing. Hidden and embedded trackers within online services record interactions with the person. The ways in which the information gathered by trackers is subsequently used are opaque to the user and may be unwelcome. An example of this was the UK Metropolitan Police's [privacy breach](#) in sharing victims' reports of sexual offences and domestic abuse plus their identities to Facebook via the Meta Pixel tracking tool embedded in their crime-reporting website.

Individual fragments of personal data shared online may seem to have minimal risk associated with them. However, linking these fragments *across platforms* and *across time* can produce a mosaic that affords significant and unintended insights into an individual's habits across their work and private life; their personality, emotions and mental health; who they hang out with and where (Armstrong et al., 2023). In extremis, such insights can impact civil liberties. This is evident in the digital authoritarianism exerted by the Chinese Communist Party, whereby AI-powered surveillance is used to enforce citizens' 'acceptable' behaviour via the compilation of social credit scores grounded in extensive personal data (Kendall-Taylor et al., 2020). Citizens with 'bad' scores can be excluded from state-sponsored benefits, such as permission to travel by air or rail. Beyond individual people, a bigger picture invites concern in national security contexts. Adversaries with malign intent can use mosaics of personal data to deduce strategic vulnerabilities with political, national and global dimensions (Pozen DE, 2005).

Personal data is persistent. It is easy to replicate, reproduce, edit and manipulate. And it is hard to get rid of once it's online or recorded digitally in one or more databases. Deletion is either not supported, is practically impossible because of technical and logistical roadblocks, or the data is so deeply entangled with other data that it cannot be extracted. For example, think of all those great photos of you with your best friend *and* their pesky ex.

Personal data is also highly accessible via search engines, which are designed to find information and make it accessible to all. One of the problems here is that information that is incorrect, outdated, or irrelevant can still be found and shared with unknown others. In the new age of generative AI, it has already been clearly demonstrated that "hallucinations" based on partial or incorrect data are being presented as "truth" and as "facts". Presented with authority, these may be based on incorrect personal information or imagined information based on inaccurate composites. The key point here is that it is almost impossible to comprehensively audit, correct, curate or delete our personal data once it has appeared online. The most optimistic outcome many hope for is that – like leaves in a pond – personal data will gradually drift into murky obscurity, failing to surface on the first few pages of a search engine over the years or to be readily dug up by LLM-managed and propelled information collation engines.

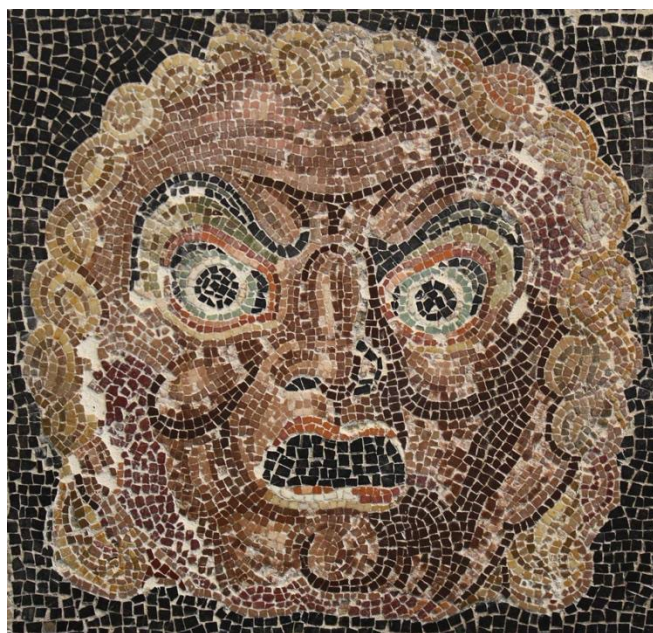


Image: <https://www.worldhistory.org/image/3221/theatre-mask-mosaic/>

#### Times of change

I/we have been researching how the issues outlined above affect everyday people and how technologies do and do not align to what they need. Our explicit interest lies in times of change. For over a decade, we have carried out privacy studies focussed on times of change, including end-of-life, relationship breakdown, leaving the military, cancer diagnosis and coming out as LGBT+ across more than a decade (Moncur, 2015; Armstrong et al., 2023).

Starting. Stopping. Joining. Leaving. Evolving. We all go through times of change in our lives. Whatever we leave behind – school, a job, a marriage, a gender identity - it's all change, and digital systems don't handle such changes well. Technological infrastructures, tools, and apps are designed well for onboarding and maintenance users. They are designed less well for supporting the natural evolution of our identities across the lifespan. When people want to change how they appear online - whether that be through more (or different) levels of privacy, the ability to edit, redact, or delete information already collected, or who they are connected to - technologies either fail them, present obstacles through the complexity of privacy management options, or (at the least) cause extra and unwanted work.

We have encountered many examples of how technological infrastructures, tools, and apps let people down in these contexts unless they have a high degree of digital privacy literacy.

When digital privacy is working as a user wishes, the use of online channels can have positive effects during times of change. Users with greater digital privacy literacy may curate their content and audiences, sharing information thoughtfully and leveraging technology to alleviate the emotional labour of change:

*"I planned carefully what and how I would share, and it has saved me having multiple and identical conversations - which gets very tiring. Before sharing, I had been ruthless in clearing out my 'friends' list to include only those I see as genuine friends and people who I wanted to know what was happening to me."* (Interviewee, living with cancer).

They may also mobilise support and find acceptance of their "new normal", regardless of what their change is:

*"Internet is full of trolls and bullies, but if you can distance yourself from that and find groups that are private and secure, then these groups are there to help..."* (Interviewee, leaving the military)

However, failure to proactively manage one's online privacy requirements during a time of change can have persistent repercussions:

*"I was foolish really by thinking what I write was floating out into the ether, but somehow disappearing amongst all the other messages, never to be seen again. I guess I thought that people could see it for a few hours, and then it was lost. Sadly, they are a little more fixed in concrete than that."* (Interviewee, relationship breakdown).

News of change can easily leak out to the wrong people, engendering unwelcome online visibility and the associated negative ramifications:

*"I thought I had shared this information anonymously [online], but I got found out by an amateur Sherlock Holmes and ever since, it has screwed my personal life up!"* (Interviewee, relationship breakdown).

Such visibility is amplified when personal data is aggregated across platforms and across time. For example, for someone living with cancer and looking for a new job, what effect might it have if a potential employer scrutinises both their LinkedIn professional profile and their publicly visible cancer fundraising biography? - are they at risk of not being hired? What is the impact on personal safety for the owner of a small business who has escaped an abusive relationship and wants to hide where they now live when the UK Government's Companies House reveals their home address as a matter of public record and lax Strava settings display their daily exercise route? - will their abuser be able to find them?

### Relationship breakdown

Now, let's dig deeper into one common time of change: relationship breakdown. Online, there may be a need to uncouple intertwined identities and adjust the networks and individuals we are connected to to reflect our new normal and who knows about it.

If the relationship has been abusive, it is vital to take steps to uncouple these intertwined identities and avoid the unwelcome sharing of personal data. Technological infrastructures, tools, and apps afford additional opportunities to transact abuse and to pursue the survivor after the relationship ends (Grimani et al., 2022). While domestic abuse takes many forms - physical, sexual, psychological, and economic - up to 72% of reported cases now also involve technology-facilitated abuse (TFDA) by perpetrators that aim to intimidate, threaten, monitor, impersonate, harass, or otherwise harm survivors (Christie & Wright, 2020). It is transacted across a wide

range of devices - including smartphones, laptops, smart home devices, and GPS – and via channels including social media and text messages, plus stalkerware, spyware, and monitoring tools.

Abusers can make it even harder for survivors to leave, seek help, or resist further harm via imposed restrictions on the survivor's digital privacy, and the exploitation of digital technologies and survivors' associated personal data. Survivors may fear reaching out for support online for fear of discovery. Personal data such as intimate images shared consensually within a relationship in happier times may be shared with a wider audience by the abuser, with the intention of causing shame or embarrassment. Location-sharing apps that once seemed like a cute way of staying in touch morph into mechanisms for intrusion and control:

*"By this stage, I had blocked him on Google because I was sick of getting his constant messages... but I didn't know that I hadn't also blocked the location services... He ...tracked me, knew I was [at an event], knew the exact time, how long I'd been there... It was really creepy. It was really terrifying as well."*

Knowledge of personal data may even facilitate economic abuse. One interviewee explained how knowledge of her email address and detailed personal identifying information enabled her abuser to carry out fraud:

*"We owned a rental property together. He took out a loan in my name online to pay for the insurance on it, so he didn't have to pay his share. I only found out by accident when I read what I thought was a spam email saying how much I owed! The police said it wasn't fraud as he was my husband – even though we were separated."*

Next steps?

Having shared some high-level framing of the mosaic of personal data and some personal examples from our research, I turn to the question of what can be done. What can we, as HCI, UX, and UxD professionals, do? Whether it is to defend against an abuser intent on TFDA or to prevent a cancer diagnosis from leaking out to undesired audiences online, digital privacy settings *need* to be easier to manage. Some steps are being taken to improve digital privacy literacy. Currently, charities such as [Refuge](#) have excellent checklists that people can use to self-audit commonly used apps and services and make them more secure.

But this isn't enough. Expecting someone who is going through a period of significant change to spend time fiddling with complex privacy settings across multiple platforms is both unrealistic and unreasonable. It's also unfair. Real life should be allowed to take priority. It shouldn't be so hard to change who we are connected to or what information they see about us, or to avoid the potential adverse consequences of failing to attend to privacy settings.

There is an opportunity here for HCI, UX, and UxD professionals to develop usable privacy-enhancing tools that nimbly assemble an individual's mosaic of personal data across platforms and across time and reflect it back to the individual so that they can understand what they reveal of themselves, and to whom. And we need these tools embedded into apps and online services. This will afford people opportunities to manage their digital privacy during times of change and to shore up unforeseen privacy vulnerabilities at a time when, frankly, people have better things to do.

#### Acknowledgements

The research reported on in this article was undertaken in collaboration with:

- Dr Jo Briggs, Manchester Metropolitan University
- Dr Lorna Gibson & Dr Aikaterini Grimani, University of Dundee
- Dr Ryan Gibson, Dr Diane Morrow, Dr Emma Nicol, University of Strathclyde
- Dr Daniel Herron, Facebook

Research funded under the following grants:

- Keeping Secrets Online, Centre for Research and Evidence on Security Threats
- Cumulative Revelations of Personal Data (EPSRC [EP/R033889/2](#))
- AP4L: Adaptive PETs to Protect & emPower People during Life Transitions ([EPSRC EP/W032473/1](#))

References

Christie, L., & Wright, S. (2020, November). **Technology and domestic abuse**. UK Parliament Post. <https://post.parliament.uk/technology-and-domestic-abuse/>

Grimani, A., Gavine, A., & Moncur, W. (2022). **An Evidence Synthesis of Covert Online Strategies Regarding Intimate Partner Violence**. *Trauma, Violence, & Abuse*, 23(2), 581-593. <https://doi.org/10.1177/1524838020957985>

Armstrong, A., Briggs, J., Moncur, W., Carey, D. P., Nicol, E., & Schafer, B. (2023). **Everyday digital traces**. *Big Data and Society*, 10(2). [https://doi.org/10.1177/20539517231213827/ASSET/IMAGES/LARGE/10.1177\\_20539517231213827-FIG1.JPEG](https://doi.org/10.1177/20539517231213827/ASSET/IMAGES/LARGE/10.1177_20539517231213827-FIG1.JPEG)

Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). **The digital dictators: how technology strengthens autocracy**. *Foreign Affairs*, 99(2), 103–115.

Moncur, W. (2015). **Digital Ownership across Lifespans**. In C. Garratini & D. Prendergast (Eds.), *Aging and the Digital Life Course* (Vol. 3, pp. 257–273). Berghahn Books. [https://strathprints.strath.ac.uk/85168/1/Moncur\\_ADLC\\_2015\\_Digital\\_ownership\\_across\\_lifespans.pdf](https://strathprints.strath.ac.uk/85168/1/Moncur_ADLC_2015_Digital_ownership_across_lifespans.pdf).

Parkinson, B., Millard, D. E., O'Hara, K., & Giordano, R. (2018). **The digitally extended self: A lexicological analysis of personal data**. *Journal of Information Science*, 44(4), 552–565. <https://doi.org/10.1177/0165551517706233>

Pozen, D. E. (2005). **The Mosaic Theory, National Security, and the Freedom of Information Act**. *The Yale Law Journal*, 115(3), 628–679. <http://www.jstor.org/stable/25047621>