



Open Research Online

Citation

Perriam, Jessamy and Copson, Lynne (2024). Poor policy made durable: when digital transformation meets social harm. In: Perriam, Jessamy and Meldgaard Kjær, Katrine eds. Digitalization in Practice: Intersections, Implications and Interventions. De Gruyter Contemporary Social Sciences, 14. Berlin, Boston: De Gruyter, pp. 141–161.

URL

<https://oro.open.ac.uk/94707/>

License

(CC-BY-NC-ND 4.0) Creative Commons: Attribution-Noncommercial-No Derivative Works 4.0

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Policy

This document has been downloaded from Open Research Online, The Open University's repository of research publications. This version is being made available in accordance with Open Research Online policies available from [Open Research Online \(ORO\) Policies](#)

Versions

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding

Chapter 8

Poor policy made durable:

When digital transformation meets social harm

Content warning: this chapter mentions self-harm and suicide.

Introduction

Shortly after 1am on the night of 14 June 2017, a fire broke out in Flat 16 on the fourth floor of a 24-storey tower block of social housing, known as Grenfell Tower, situated in North Kensington, London, UK. While the immediate cause of the fire was attributed to an electrical fault with a fridge freezer, a number of contributing factors to both the spread of the fire and its impacts have also been identified. These included cladding that had been added to the tower block which was found not to meet Building Regulations; the failure of London Fire Brigade (LFB) to provide an evacuation plan for a high-rise building along with lack of training and a ‘failure to appreciate the nature of the risks posed by the cladding at Grenfell Tower’ (Grenfell Tower Inquiry, 2019: 590), and deficiencies in LFB policies relating to the management of emergency calls (Grenfell Tower Inquiry, 2019).

The harms of the Grenfell Tower fire are far-reaching and many of them are not captured by conventional criminal justice or legal processes. In addition to failures (of electrical goods, cladding or policies) that resulted in the fire, a zemiological (or social harm) approach turns attention to the broader social context in which such apparently discrete ‘accidents’ or ‘failures’ are situated. For example, the Royal Borough of Kensington and Chelsea in which Grenfell Tower is located, is the richest borough in London, itself one of the most expensive cities in the world. Meanwhile, a closer analysis reveals the specific area in which Grenfell Tower was located – Notting Dale Ward – ‘was among the top 10% most deprived areas in England in 2015’ (Barr, 2017). Despite its wealth, the local authority was accused of using a ‘cheaper quality cladding material’ (Watt, 2017) that is banned from use in tower blocks in other European countries and was found to have facilitated the fire’s spread ‘to save an estimated £290,000’ (Watt, 2017). This led to claims that the local authority was more concerned with the cosmetic appearance of the tower and finances rather than the safety of those living within (Booth, 2020). Furthermore, despite residents’ concerns regarding fire hazards being raised to the council on numerous occasions no action was taken, leaving residents ‘powerless in their attempts to improve the safety of their homes’ (Watt, 2017).

In this chapter, we explore and develop the social harm perspective that has been used to analyse the events of the Grenfell Tower fire by applying it to case studies of digital transformation. In doing so, we not only seek to demonstrate the potential harms of digital transformation – many of which are unaddressed and unaddressable by legal recourse – but, through this analysis, argue that these cases present clear examples of how poor – and harmful – policies are made durable through digital transformation.

When we interact with public services in digital settings, we generally experience some form of convenience. We did not have to stand in line at the post office to apply for our driving licence and we did not have to fill in a paper form to file a tax return for the previous financial year. We no longer interact with a human intermediary to complete these bureaucratic tasks.

But with increased convenience comes increased trust that these digitised services are accurate and that they represent citizens in a way that will not inadvertently penalise them in error. For example, we trust that the tax department holds accurate data on its taxpayers and understands the algorithms applied to that data to calculate someone's tax liability. We trust that welfare systems will clearly explain to citizens what is required of them when they interact with digitised systems for accessing benefits along with a clear reasoning for these requirements.

While citizens have these expectations, there are instances where they are not met. In recent years, there have been reported examples of failures of digitised government systems which have directly harmed citizens. How are we to investigate the responsibility and accountability in situations such as these where citizens have been harmed but criminal intent can be difficult to pin down?

In this chapter, we describe social harm – or *zemiology* – and how it has developed in response to criminology to articulate situations where citizens have encountered avoidable harm but where it is difficult to connect that harm to a particular law, precedent or individual. This leaves citizens worse off than before they encountered the harm and crucially, with little or no recourse to accountability or compensation.

We unpack the relevance of social harm by first describing the theory in more detail and demonstrate how it has been used in the past to illuminate the social impacts of government and commercial decisions, using the Grenfell Tower fire as an example. We then describe how public sector digital transformation has taken place in the UK, along with the motivations for doing so. We then apply the concept of social harm to three cases in digitised services; the Post Office IT case in the UK, the failure of 'Robodebt' in Australia, where social security payments were checked against tax declarations by an automated system to check whether Australian

taxpayers owed the government money, and the UK's Universal Credit system as articulated in Alston's 2019 UN Special Rapporteur on Poverty report.

Situating digital transformation

To get a better understanding of these case studies in relation to social harm, it is necessary to briefly outline the history of digital transformation of public services in the UK. From the outset, it is important to note that public sectors in many nation states have incorporated some form of computerisation for many decades. The importance has been to consider what tasks have become digital and who has had to interact with technology to achieve the task they set out to complete.

The UK has had multiple waves of digital transformation since the rise of computing in the post-World War Two era. As Mar Hicks (2017) outlines, the UK's computing industry was influenced and supported by developments from war activities primarily occurring at Bletchley Park, processing large volumes of data at an increasingly faster rate to aid in codebreaking efforts to secure intelligence for wartime operations. With a transition to peacetime, the need for this particular use of computing power became unnecessary and attention shifted to repurposing these tools and skills. Notwithstanding commercial use cases, the British government made use of the technology, especially in the then-publicly owned Post Office, which was also responsible for telecommunications. Hicks also describes how this technology was incorporated into processing data within government departments post-World War Two. This was done with the co-operation of companies that the government owned or invested in. However, in the 1970s, the UK economy took a downturn and government investment in computing technology and staffing decreased and previously protectionist policies that kept the British computing industry going were relaxed, allowing international competitors into the market. The government effectively became a customer rather than a creator of technology. During the 1980s and 1990s, many government data processes were put out to commercial tender, rather than being built and maintained in-house. During this era, it was standard practice for the government to sign 10-year contracts with providers, with extra payments necessary to perform updates and maintenance tasks. These services formed the technical backbone of many government departments. However, it is important to note that citizens rarely directly interacted with these systems. They were the end beneficiary, but not the end user. Rather, government employees were primarily interacting with these systems to carry out tasks such as data entry and processing on behalf of citizens. If there were issues with the system, the person who was

interacting with the system had the expertise and ability to verify, rectify or modify the problem.

With the advent of the mainstream internet era in the 1990s, there were growing calls for the UK Government to have an online presence. The early years of this transition online have been thoroughly covered by Jerry Fishenden (2014a, 2014b, 2014c) in his online archive. The first government websites were initially created purely to provide government information for citizens online, but as the internet advanced there was increased interest in allowing citizens to use the technology to carry out government transactions. This shift has the ambition of making citizen-government transactions go from paper to digital.

The reality is much more complicated than just shifting citizens to a new format. With it, comes both a learning curve of digital literacy for citizens to be able to interact with government online and, an assumption of the economic means to access both the tools and infrastructure essential to complete the necessary transactions. From the government side, the challenges lie in maintaining the technology and working with citizens who do not fall within the expected use cases of these digitised transactions.

In the race to make many government transactions digital – often due to government departments being seduced by the greatly reduced cost per transaction of digitised services – there have been oversights that could easily be rectified by human intervention, but instead become larger problems, often with harmful consequences for citizens. The remainder of this chapter will unpack social harm as a concept and apply it to some large-scale government IT failures in the UK and Australia.

Digital transformation in Australia

Within the Australian context, the digital transformation that occurred in the 2010s with the establishment of the Digital Transformation Office (DTO) (now the Digital Transformation Agency) in 2015. The rationale for digital transformation was somewhat similar to that of the UK, with a focus on bringing all federal government transactions under one central website. Many of the senior staff involved in the establishment of the DTO were former senior staff at the UK's Government Digital Service, hired specifically to bring their expertise to bear in the Australian context.

In practice, there are some differences in the Australian digital transformation landscape. The first is that Australia has three levels of government in comparison to the UK's two levels of government. This adds a layer of complexity and stakeholders to digital transformation activities and requires citizens to know which layer of government is responsible for the

transaction or information they require. The second difference is that the Australian government has opted to conduct government transactions and send some notifications through the MyGov portal. This is similar to Denmark's DigitalPost and borger.dk systems with the crucial difference that citizens choose which government services they access through MyGov. The Covid-19 pandemic saw an acceleration of digital transformation through apps, with many states developing apps with the initial idea to cover identification and verification during the pandemic to then pivot into non-pandemic related functions. There are also calls to have identity and data services between states and the federal government become shareable or interoperable (Department of Finance 2022a, 2022b).

Introduction to social harm

Zemiology (also known as a social harm perspective or approach) emerged relatively recently as a contribution to social enquiry that seeks to move beyond what are perceived as the limited confines of crime, criminology and criminal justice approaches to identifying, analysing and, ultimately, addressing harmful social phenomena. Broadly defined as 'the holistic study of harmful social phenomena, encompassing, but not limited to, physical, financial, psychological and cultural harms' (Copson, 2021: 170), more recent analyses have also added to these harms of recognition, autonomy harms, and temporal harms (Canning and Tombs, 2021: 78). Zemiology both derives from and is critical of criminology in general and critical criminology in particular, for their role in constructing a particular and limited view of harm.

Underlying much of the criticism of existing criminological paradigms and legal remedies is a critique of the power relationships underpinning these systems, reflecting and reinforcing the unequal status of different actors (Hillyard and Tombs, 2004: 17-18). Indeed, this is an issue to which critical criminologists have long sought to bring attention (see Copson, 2021: 17). Most notably, they have pointed out that the avoidable harms resulting from the routine practices of powerful actors, such as states and corporations, tend not to result in the same types of penalties or moral outrage (assuming they result in any) as interpersonal crimes conducted by low status individuals.

However, zemiologists are critical of the discourse of crime and any attempts to understand and address harms that implements this discourse, including those of critical criminologists. They argue that the discourse of 'crime' constructs particular harms in particular ways which, in turn, influences the types of recourse that are available when such harms occur. Specifically, they point out how the discourse of crime often struggles to recognise harms which do not result from discrete, intentional acts or omissions by identifiable individuals and shapes those

harms it does recognise within this framework – focussing on the actions and behaviours of individual actors rather than broader social structures and processes in which they are frequently situated (see Copson, 2021; Hillyard et al., 2004).

By contrast, zemiology presents a tool for imagining the world and social processes differently – by situating individual experiences of apparently discrete harms in a broader context that both recognises the multi-dimensional nature of such harms and allows more holistic, joined-up thinking about their causes, impacts and how best to respond to them (see Copson, 2021; Canning and Tombs, 2021).

Steve Tombs has applied the zemiological perspective to the Grenfell Tower fire to highlight the multi-dimensional experiences of harm it entailed, in addition to the lives lost. Tombs notes that these harms would likely have included:

- *Physical harms* – the obvious physical harms of death and injury to survivors, but also less apparent forms of physical harm. These could include ‘airborne toxins [that] might have been emitted as a result of the fire’ (Tombs, 2017: 68) and have a lasting impact, and the exacerbation of drugs and alcohol dependency and prior existing health conditions (such as heart disease, obesity and diabetes) which become harder to manage in the temporary accommodation in which survivors were placed (ibid.).
- *Psychological and emotional harms* – Tombs notes that ‘within a few months of the fire it was estimated by Grenfell NHS that “at least 11,000” people would need long term mental health treatment as a result of the fire’ (2017: 70) and ‘at least 20 survivors and witnesses of the fire had attempted to take their lives within 3 months of it,’(ibid.). These harms are not limited solely to those who lived in Grenfell Tower, having the potential to impact loved ones of those affected, witnesses and residents of similarly-designed buildings (Tombs, 2017: 71).
- *Cultural harms* – defined as ‘harms produced by having the ways of living to which [people] are accustomed or acculturated either disturbed or, literally, removed’ (Tombs, 2017: 72.), the physical relocation of survivors resulted in the loss of ‘networks, mutual supports and common experiences’ (ibid.) that were central to their lives.

- *Harms of mis-recognition* – harms of mis-recognition are highlighted by the disregard experienced by residents of Grenfell Tower from the local authority and the Kensington and Chelsea Tenants Management Organisation (which was responsible for the building), as evidenced by its failure to heed their warnings and conscious decision to put cost over their lives (Tombs, 2017: 73-74).
- *Financial and economic harms* – funeral and memorial expenses, travel expenses to/from temporary accommodation, lost wages through inability to attend work, costs of replacing goods where insurance was non-existent or inadequate, food costs in temporary accommodation with limited food preparation facilities represent some of the financial harms experienced (Tombs, 2017: 76-77). Further harms include the costs to the local authority – of responding to the fire, legal fees and any subsequent fine, and the costs of setting up the Public Inquiry, which will ultimately be borne by citizens through either taxation or cuts to essential services, which will disproportionately impact the most vulnerable (Tombs, 2017: 77-78).

While a focus of crime allows only a ‘snapshot’ of an intentional act or acts’ (Tombs, 2017: 62) and focusses on demonstrating a direct causal link between criminal intent and harm, the advantage of the social harm approach is its capacity to recognise the widespread and disparate impacts of seemingly discrete instances of harm in a wider social context – both in terms of understanding their causes and their impacts.

We contend that the zemiological perspective can offer a useful framework to analyse digital transformation and to challenge dominant discourses that assume the benefits and downplay their harms. In doing so, we seek to demonstrate how digital transformation is complicit in making poor – and harmful – policy durable. This is particularly evident in the context of what Charles Perrow (2011: 3) calls ‘high-risk technologies’. These are systems ‘that increase the risks for... operators, passengers, innocent by-standers, and for future generations’ (ibid.) of experiencing (often catastrophic) harm. Typically, this capacity for harm is built-in to the systems themselves and they have the potential to impact thousands or millions of lives quickly and directly (ibid: 3-4). The case studies we have selected to focus upon can be considered examples of just such ‘high-risk technologies’. In the next section, we turn our attention to outlining these case studies of digital transformation that we explore through the lens of social

harm to highlight the current systemic limitations for recognising and addressing these harms through conventional legal recourse. These cases are selected based on the authors' familiarity with them that have received a significant degree of reporting in English-language media outlets. This allowed the gathering of anecdotal evidence documenting the range of harms reported by those who had been directly involved in the cases.

Case studies of digital transformation and social harm

Much of the discourse around digital transformation centres on the promise of swifter bureaucracy, cost-savings and the benefits for citizens and authorities alike. Meanwhile, a great deal of the countering discourse focuses on those left behind by digital transformation and is often discussed with the terms 'digital inclusion' or 'access'. However, when we talk about social harm and digital transformation, we are considering something beyond a citizen's ability to use a digital service. We are talking about times where a digital system fails a citizen with detrimental consequences, where the system is agnostic about the citizen's ability and/or risk is 'built-in' to the system. In some cases, the citizen may not even be aware of the digital system's existence until they are impacted by its output. Two high profile examples of this include the Post Office IT scandal in the UK and the 'Robodebt' case in Australia. Both examples involve situations where citizens are wrongly accused of fraud due to technical errors that went unchecked.

Post Office IT failure and undermining of community trust

Post Office workers in the UK are considered upstanding members of the local community. They handle mail, help you to pay bills and undertake other essential transactions, such as passport applications. Following the separation of the Post Office Ltd from Royal Mail in 2012, many Post Offices are now run as franchises; with franchisees formally called subpostmasters. In the early 2000s, the Post Office IT contractor, Fujitsu introduced a new IT system called Horizon, which was built to keep track of the sales and accounts undertaken at each Post Office branch. However, there were errors with the Horizon system, showing shortfalls in the accounts of individual franchises, often running into thousands of British pounds (Thomson 2009). Post Office management thought these discrepancies were due to subpostmasters defrauding the Post Office of money, similar to a cashier taking money from a cash register. As a result, 736 subpostmasters were charged and convicted for theft, fraud and false accounting between 2000 and 2014 (Peachey, 2022). In reality, the shortfall figures were due to errors in the accounting system left unchecked despite calls from subpostmasters for Fujitsu to investigate and address

the problems. Some of those convicted in relation to these errors spent time in prison, went bankrupt or had family or relationship breakdowns. Four subpostmasters took their lives while waiting for intervention from the legal system (Witherow and Trump, 2021). In 2019, the High Court found in favour of the subpostmasters and ordered that the Post Office pay compensation to the claimants. Some subpostmasters also had their fraud convictions overturned (Peachey, 2022).

A simple error causes errant welfare fraud notices

While subpostmasters in the UK were dealing with false fraud allegations, Australian citizens were dealing with a Debt Recovery Scheme that erroneously stated that they had an outstanding debt to the government. Dubbed “Robodebt” (Henman 2017), the scandal arose after the implementation of software that automated the detection of debt and fraud in Australia’s welfare benefits system. Not only did the system detect fraud, it automatically sent debt collection notices to citizens that had been identified by the system. The use of data matching to detect fraud in and of itself is not illegal (it has been legal to do this in Australia since 1990), but basic errors in the detection system meant that some citizens were being sent debt collection notices based on incorrect debt calculations (Human Rights Law Centre, 2021).

The Robodebt system relied on figures from citizens’ yearly (and often automatically generated) tax declarations and their payslips. The problem arose due to the names of companies listed in the system. In Australia, you can register a company name and have many businesses listed beneath it. In practice, this means that the company that is paying you could have a different name from the business you work for, for example the overarching company could have been called ‘John Smith Ltd.’ and the workplace might have been called ‘Smith’s Sliced Bread’.

Because Robodebt depended on matching and comparing data from different systems, it created the possibility that, in one system a person could be listed as paying tax on income from the business, while in another system they could be listed as receiving their salary from the overarching company. To the system, it would read as the citizen receiving double their actual income, with identical amounts coming from the same source. This perceived doubling in income triggered the Robodebt system to consider the citizen to be fraudulently claiming more welfare payments than they were entitled to due to having too much income.

Citizens were sent notices claiming that they were paid too much and ordered to repay the outstanding amount calculated by the system, often in the tens of thousands of dollars (Henrique-Gomes, 2019). However, they were given little or no avenue to dispute the notice.

According to Henman (2017) and Knaus (2017), citizens were only able to dispute repayment notices through an online form, with frontline staff instructed to deflect calls for assistance. Many citizens receiving this notice felt they had no option but to pay the charge, despite believing it was sent in error. Many were also not in the financial position to pay what the government claimed they owed and were placed under economic, social, and psychological stress as a result. Similar to the Post Office IT scandal, some citizens who received repayment notices took their own lives as a result of the stress.

The use of Robodebt was successfully challenged through a class action lawsuit and the Australian Government stopped using the Debt Recovery Scheme in 2020, but there was also social harm incurred through this scandal. In terms of social impacts, affected individuals experienced shame following the accusation of fraudulent behaviour (Medhora, 2019). On a societal level, the Robodebt case undermined public trust in the working order of government bureaucracy. This would be true for those on the conservative side who actively believe that the government should pursue citizens over debts, because the case represents a failure in delivering public infrastructure. On a more left-wing perspective, those who do not support an aggressive debt recovery system from the government would find that a case such as Robodebt represents government overreach, obfuscation and an evasion of responsibility when systems fail to the detriment of citizens.

Digital transformation of welfare initiatives and decreased in-person support

In 2019, the United Nation's Special Rapporteur on Poverty, Philip Alston investigated the digital transformation of welfare states around the world. In his report, Alston singled out the Universal Credit system¹ in the UK as preventing eligible citizens from accessing welfare payments due to the complexity or inaccessibility of the digital-by-default system that was all but mandatory to use in the application process.

Lack of accessibility and government assistance to access Universal Credit was raised in Alston's report. Alston's report, reveals how increased, forced digital transformation of welfare provision can create social harm for both people in need of welfare and those who are informally helping them, through a system that actively discourages officials from giving assistance. It also perpetuates destitution and creates a range of mental, physical and social

¹ Universal Credit is a welfare reform in the UK engineered in 2010 by then coalition Government minister of the Department for Work and Pensions, Iain Duncan Smith. The concept of Universal Credit is that rather than receiving multiple, separate payments from the government such as Child Support, Job Seekers' Allowance, etc, these payments would be rolled into one payment that often amounts to the citizen receiving less money, placing them further below the poverty line.

flow-on effects for those who cannot economically participate in society due to the difficulties in their daily cost of living.

Unlike the Robodebt and the Post Office IT cases, as yet, there do not appear to have been the same types of direct legal challenges to the Universal Credit online system. At time of writing, legal firm Leigh Day are the process of pursuing a group action pertaining to changes that were made to payment of severe disability premiums following the change to Universal Credit (Leigh Day, 2022). However, as this action demonstrates, cases relating to the Universal Credit are typically concentrated upon or also bound up with more general issues relating to decisions and policies Universal Credit, rather than the digitised system itself. This may reflect both the relative powerlessness of claimants against the state, as well as how the system and the policy are intertwined.

That said, it is notable that in the Robodebt example, initially cases were dealt with as individual ‘blips’ in the system, before the volume of cases meant the problems of that system itself could no longer be ignored (Whiteford, 2021). This may also end up being the case with Universal Credit. By contrast, in the Post Office IT case, the digital system was much more clearly identifiable as the source of the harm. Nevertheless, in all three cases, anecdotal evidence demonstrates how citizens have suffered a variety of social harms because of ‘high-risk technologies’ (Perrow, 2011) of digital transformation. It is to exploring these harms that we now turn.

The social harms of digital transformation

Building on Tombs’ application of a typology of social harm to the case of the Grenfell Tower fire, a similar application to the case studies outlined here, reveals similarly wide-ranging harms associated with such cases of poorly executed and maintained digital services that cannot be recognised or addressed within existing channels.

Financial harms and economic harms

In all three of the Post Office, Robodebt and Universal Credit cases, instinctively financial and economic harms seem the most prominent. As a welfare policy aimed at providing financial support for some of the most vulnerable in society, financial harms are especially prominent in the Universal Credit example, with examples of citizens denied much-needed financial assistance in a timely manner due to an inability to access the system. In one such case, a 61-year-old woman with a learning disability had her benefit cut, losing out on nearly £1000 to which she was entitled, after she failed to respond to a note on her account. Receiving support

from a charity worker who advised the Department of Work and Pensions (DWP) that the woman was unable to read and access her online account, the DWP reportedly responded that, as an online service, they ‘do not communicate by letter’ and advised that the online system would have to be updated (Booth, 2019).

Meanwhile, in both the Post Office IT and Robodebt cases, individuals were left trying to find money they were told they owed which they often did not have. People lost jobs and regular income. In one case, a subpostmaster pled guilty to four counts of fraud, resulting in a fine of £14,000 because she assumed that she must be doing something wrong and ‘did not want to go to jail and leave behind her daughter, who was 10 at the time’ (Bennett, 2022). Elsewhere, as a result of the Robodebt scandal, another person wrongly accused found themselves having to move back in with their parents when faced with the prospect that they owed the government \$6,000 (Henrique-Gomes, 2020a). Such issues demonstrate the broader harms engendered by what appear, superficially at least, to be primarily issues concerning money, which is evident across all three cases.

Physical harms

Despite their digital and financial nature, families of both those involved in the Post Office IT and Robodebt cases have claimed significant physical harms have resulted for those involved, including health conditions brought on by stress, premature death, and suicide (Peachey, 2022; Henriques-Gomes, 2020b). Bearing in mind that many Universal Credit claimants may already experience problems with their health and/or disability, the Universal Credit system has also been found to exacerbate already existing physical health conditions (Cheetham et al., 2018: 25) through, for example, increasing food insecurity (ibid.: 23). Further, an inquest found the stress caused by completing the application for Universal Credit to be connected to at least one self-inflicted death, that of Mark Jacka, who had dyslexia and reportedly struggled to complete the required forms (Rethink Mental Illness, 2021: 10).

As with survivors of the Grenfell Tower fire, there have also been concerns about an increase in addiction or substance dependency amongst those involved in the Post Office IT scandal, along with high blood pressure (Ambrose, 2022), and alopecia (Bennett, 2022). For Universal Credit claimants, it has been reported that sanctions have been associated with increased substance misuse, self-harm and suicidality (Cheetham et al., 2019: 6-7).

Physical harms in these cases were not limited to those directly implicated. In the case of the Post Office IT scandal, self-harm amongst children of those accused was reported (Bennett, 2022) while the imprisonment of those wrongly accused led to the physical separation of

families and included the imprisonment of those who were pregnant, amongst others (Peachey, 2022). Similarly, although the physical harms of the Universal Credit case are perhaps most immediately experienced by the recipients of the benefit themselves, Universal Credit workers have reportedly been advised to avoid disclosing that they work for Universal Credit to ensure their own safety (Thorp, 2019).

Psychological and emotional harms

The overlap between physical and psychological and emotional harms is particularly striking across all three cases.

The failures of the Universal Credit system and its challenges are documented as contributing to high levels of stress, low self-esteem, depression, anxiety and suicidal feelings amongst claimants (see Booth, 2019; Cheetham et al., 2018: 23-25). Emotional distress has also been experienced by Universal Credit workers, who are tasked with having to support often distressed, desperate and suicidal claimants through the system (Thorp, 2019). One worker has reported ‘struggl[ing] with her own feelings about herself’ (ibid.) due to her role in making decisions around people’s claims, describing the job as ‘stressful, mentally and emotionally draining, and the worst thing I feel I can do to someone’ (ibid.).

Indeed, significant psychological and emotional harms have emerged in all the cases of digital transformation we explore, resulting in mental health conditions such as PTSD and depression, as well as exacerbating conditions for those already living with them. As part of the Independent Inquiry into the Post Office IT scandal, one worker reported how she had considered and researched how to take her own life as well as suffering from PTSD and depression (Ambrose, 2022). Another ‘told how he suffered a mental breakdown, turned to alcohol and attempted to kill himself several times before being admitted to a mental health institution’ (ibid.).

Again, these impacts are widespread, often affecting the families of those directly accused. In the UK, children of accused subpostmasters experienced bullying (Bennett, 2022) while those who lost loved ones to suicide in deaths attributed by families to the Robodebt scandal experienced grief (Henriques-Gomes, 2020b).

Cultural harms

The cultural harms in such examples are also widespread. The threat of owing money and an inability to pay can have profound impacts to participate fully in society through the loss of homes and threat of imprisonment. Indeed, those who were imprisoned because of the Post Office IT scandal lost many of the basic freedoms essential for participating fully in social and

cultural life. Meanwhile, at least one Universal Credit claimant who had been released from prison was reported to have been unable to ‘cope with the system and said he wanted to go back inside’ (Booth, 2019). His inability to engage with the system led to him ‘kicking off’ for which the police subsequently arrested him (Booth, 2019).

In all three cases, people experienced job loss and/or financial insecurity, thereby hampering their ability to participate fully in key aspects of their routine, normal life. For example, one Universal Credit claimant did not receive a benefit payment due to him following an automated reporting error relating to his income which Jobcentre staff were unable to correct. He reportedly ‘ended up homeless and estranged from his family’ (Booth, 2019) as a result. Meanwhile, in the case of the Post Office IT scandal, families were reportedly rent asunder through imprisonment, marriage breakdown and premature death (Peachey, 2022), as well as bullying and other forms of exclusion. One victim of the Robodebt scandal describes feeling as if they ‘got put back a couple of years in life’ (Henriques-Gomes, 2020a), while a former subpostmaster similarly feels as if he has lost 10 years of his life ‘doing menial jobs which are massively beneath [him]’ (Bennett, 2022).

Harms of mis-recognition

Perhaps one of the most profound and yet intangible harms caused in these cases were those of mis-recognition. Previously upstanding members of the community in both the Post Office IT and Robodebt cases found themselves recast and stigmatised as poor citizens, unreliable, dishonest and untrustworthy. This was most notable in the Post Office IT scandal, where subpostmasters hold a position of relative privilege and are expected to be upstanding members of the community. Subpostmasters found themselves labelled within the communities they had lived and served as liars and thieves and held responsible for the closing of local services, such as the Post Office (Ambrose, 2022). Others reported feeling stupid because they couldn’t make sense of the (incorrect) data (Bennett, 2022) and worthless (Ambrose, 2022). As one subpostmaster who received a suspended prison sentence reported, ‘I visited the area [where the Post Office he managed had been] with my wife and we were basically told: ‘We shouldn’t be speaking to you, we shouldn’t talk to you, we shouldn’t be seen to be talking to you’ (ibid.). Universal Credit claimants reported feeling as if they were ‘not trusted or believed by DWP staff’ (Cheetham et al., 2018: 24) when they tried to explain the problems they were experiencing with the system and the impact this had on their mental health. As noted above, the inability to navigate the system can be particularly challenging for those with learning disabilities, dyslexia, functional illiteracy or irregular internet use. One such claimant,

described how he felt the system ‘assess[es] you as a number not a person. Talking is the way forward, not a bloody computer. I feel like the computer is controlling me instead of a person. It’s terrifying.’ (Booth, 2019).

At this stage, it should be noted that the application of the social harm approach above is not exhaustive and is intended only as a heuristic device to help demonstrate how the zemiological perspective can facilitate a more nuanced understanding of the widespread harms digital services can perpetuate and produce.

Making poor – and harmful – policy durable

As these examples demonstrate, in various ways, the harms of digital transformation are frequently multifarious, widespread and overlapping: predicated on an assumption of citizen’s digital literacy combined with a misplaced belief in the infallibility of digital systems in contemporary culture. These beliefs reinforce the assumption that this kind of literacy and these systems are a cultural norm. In doing so, however, they not only fail to recognise the fallibility of these systems but also fail to recognise the diversity of human experiences and needs or the potential impacts of digitisation along with significant implications for cultural participation, financial security, as well as physical and mental health.

They also render explicit the limitations of formal systems of accountability for recognising and addressing these harms since such harms are often seen as the ‘normal’ risks of such high-risk systems (Perrow, 2011).

In both the Post Office IT and Robodebt cases, despite recourse to legal interventions, victims remain dissatisfied in formal legal responses. Many of those affected by the Robodebt scandal were excluded from the class action ² and are further frustrated that it was settled out of court, ‘angry that a scandal they see as being punctuated by continual cover-up and obfuscation never made it to a courtroom’ (Henriques-Gomes, 2020a). As one such victim, Nathan Kearney, put it: ‘I wanted to know why those ministers felt that it was appropriate to use this illegal system and to target the most vulnerable people’ (cited in Henriques-Gomes, 2020a).

Similar suspicion is evident in the Post Office IT case, although this did reach a formal Public Inquiry. As one former Post Office Manager stated: ‘I want some decent money, a decent apology and I want there to be convictions for the people who have perpetuated the whole

² Although there has been a Robodebt class action lawsuit completed in September 2021, a Royal Commission (‘the highest form of inquiry on matters of public importance’ in Australia) commenced in August 2022 and is expected to be completed in April 2023.

conspiracy inside the Post Office. You know everyone from the top down knew and were pushing the charges' (Bennett, 2022).

In both cases, there is a striving for the type of accountability that is usually the preserve of legal systems, but also a sense that the legal avenues and compensations pursued do not fully recognise or address the harms experienced. At the same time, there is equally evidence that the problems raised by these cases is seen as being systemic rather than individual – attributable to both the functioning of the organisations and the systems they use, as well as broader patterns of inequality and power, as well as the presumed infallibility of digital processes, that left those most vulnerable unable to challenge the account of the powerful organisation or state.

For example, in the case of the Post Office IT scandal, subpostmasters regularly raised concerns about the accuracy of the Horizon system but instead of accountability and a solution, they faced fraud and theft charges (Wallis, 2022). In the Robodebt scandal, citizens were unable to find an appropriate communication channel to correct the erroneous fraud allegations to the extent that accountability was designed out of Robodebt and the only form of recourse was a class action lawsuit. Meanwhile, with Universal Credit, little thought was given to how claimants with limited means could meaningfully access the digital services that could help them get by in everyday life.

However, it is, perhaps, the Universal Credit case that reveals most acutely both the limitations of the legal system for recognising and addressing harms, as well as the role of digital transformation in making poor – and harmful – policy durable, particularly in the context of increasing high-risk technologies. It is important to note that many of the harms of Universal Credit identified in our discussion seem to be articulated primarily in terms of the harms of the system more generally rather than the digital system per se (though this digital system is often identified as a problematic element of the wider system). Indeed, it is often difficult to separate the harms of the broader policy and process from those of the digital system discretely as they are in many ways intertwined. For example, the workers who deal with distressed claimants have to handle the distress caused by failures of payment irrespective of whether this is the result of an inability to access the system or a decision that has not gone in the claimant's favour.

The example of Universal Credit demonstrates how difficult it can be to isolate the cause of these harms in the digital system itself as opposed to the broader policy of Universal Credit and its associated decision-making processes, within which the digital system is based. This is likely reflected, we would suggest, in the difficulties in raising a legal case against the digital aspects of the system in abstract from the broader policy, and hence the value of the social

harm approach to understand how apparently isolated instances of harm are often part of bigger systems. It also demonstrates acutely how digital technologies are used to make poor – and harmful – policies durable and, as such, cannot and should not be abstracted from those broader policy processes in which they are situated.

When public services are made digital, there has often been more concern for the function, usability and security of the service rather than a concerted effort to consider the socially harmful consequences of digital public services or minimise these risks. These concerns can be easily identified and mitigated with the use of professionals such as developers, cybersecurity specialists, designers and user researchers. However, there is little professional concern for social harm when public services are made digital and, as a result, an implicit contempt for, and fundamental mis-recognition of, service users. We suggest that this is an example of poor – and harmful - policy made durable.

Crucially, these failures of digital welfare provisions have the potential to cause a range of harms, including causing significant damage a person's ability to participate fully in society. Meanwhile, the failures to recognise the harmful impacts of these policies and to provide appropriate and meaningful means of redress through legal recourse reinforce the durability of the system – with any errors presented as discrete, individualised 'glitches' rather than fundamental systemic failings. In a system that all too easily obscures them, we argue, it is important to recognise the human cost of poorly delivered or maintained digital transformation products.

Conclusion

From the case studies presented, combined with the description of social harm, we suggest that digital transformation conducted without attention paid to maintenance or alternative, non-digital access methods constitutes a public issue that causes social harm to citizens that are impacted by digital or IT failures. While many of those impacted are socially or economically vulnerable as is the case in the Universal Credit case, examples such as the Post Office IT or Robodebt cases demonstrate that any citizen can be negatively impacted by unrectified errors in digital transformation – though the ability to withstand or resist these is equally determined by one's relative power vis-a-vis the organisation whose definitions they are contesting.

We suggest that when public sector services are digitised or policymakers plan to develop digital services based on new policies, that there is an accountability and maintenance clause placed into contracts with external suppliers or included as part of the service standard for those developed in-house. This clause should ensure that there is an easily accessible, non-digital

method of completing a transaction for those who cannot do so online. But more crucially, this clause should address the government's concern for system failure, prioritising a diagnosis and fix for a system when it delivers incorrect results. Applying social harm theory to the citizen impacts of digital transformation is novel and crucially, it is theory that can help us illuminate how some digital transformation projects constitute poor – and often harmful – policy made durable. It also provides a means of problematising digital systems and failures as a matter of public interest and concern rather than simply the 'collateral damage' of twenty-first century living. In doing so, it facilitates the development of a more democratised public discourse by providing a conceptual framework through which we can challenge uses of state power and question the interests it serves. We believe that incorporating a social harm mindset to the production and maintenance of state digital services is a core priority in avoiding future instances of social harm such as those endured by Australian citizens and British subpostmasters.

References

Alston, P. (2019) *Visit to the United Kingdom of Great Britain and Northern Ireland: Report of the Special Rapporteur on extreme poverty and human rights*. Human Rights Council A/HRC/41/39/Add.1. United Nations. Available at: <https://undocs.org/A/HRC/41/39/Add.1> (Accessed: 9 September 2020).

Ambrose, T. (2022) ‘“They ripped the life out of me”: ex-Post Office staff tell inquiry of stress of IT scandal’, *The Guardian*, 18 February. Available at: <https://www.theguardian.com/business/2022/feb/18/ex-post-office-staff-tell-inquiry-of-stress-of-it-scandal> (Accessed: 8 August 2022).

Barr, C. (2017) ‘Wealth and poverty sit side by side in Grenfell Tower's borough’, *The Guardian*, 15 June. Available at: <https://www.theguardian.com/uk-news/2017/jun/15/wealth-and-poverty-sit-side-by-side-in-grenfell-towers-borough> (Accessed: 8 August 2022).

Bennett, I. (2022) ‘Post Office IT scandal: Subpostmistress falsely convicted of fraud tells Horizon inquiry the experience caused daughter to self-harm’, *Sky News*, 15 February. Available at: <https://news.sky.com/story/post-office-it-scandal-subpostmistress-falsely-convicted-of-fraud-tells-horizon-inquiry-the-experience-caused-daughter-to-self-harm-12542708> (Accessed: 8 August 2022).

Booth, R. (2019) ‘Computer says no: the people trapped in universal credit’s “black hole”’, *The Guardian*, 14 October. Available at: <https://www.theguardian.com/society/2019/oct/14/computer-says-no-the-people-trapped-in-universal-credits-black-hole> (Accessed: 14 October 2022).

Booth, R. (2020) ‘Grenfell architect says cladding focus was on appearance and cost’, *The Guardian*, 11 March. Available at: <https://www.theguardian.com/uk-news/2020/mar/11/grenfell-architect-says-cladding-focus-was-on-appearance-and-cost> (Accessed: 8 August 2022).

Canning, V. and Tombs, S. (2021) *From social harm to zemiology*. London; New York: Routledge.

Cheetham, M., Moffatt, S. and Addison, M. (2018) “It’s hitting people that can least afford it the hardest” *the impact of the roll out of Universal Credit in two North East England localities: a qualitative study*. Gateshead Council. Available at: https://www.gateshead.gov.uk/media/10665/The-impact-of-the-roll-out-of-Universal-Credit-in-two-North-East-England-localities-a-qualitative-study-November-2018/pdf/Universal_Credit_Report_2018pdf.pdf?m=636778831081630000 (Accessed: 26 October 2022).

Cheetham, M., Moffatt, S., Addison, M. and Wiseman, A. (2019) ‘Impact of Universal Credit in North East England: a qualitative study of claimants and support staff’, *BMJ Open*, 9, e029611. <https://doi.org/10.1136/bmjopen-2019-029611>.

Copson, L. (2021) ‘Beyond criminology: taking harm seriously’ in Gordon, F. and Newman (eds), *Leading works in law and social justice*. London; New York: Routledge. pp. 169-190.

Department of Finance (2022a) *Data and Digital Ministers Meeting Communique 4 November 2022*. Available at: <https://www.finance.gov.au/publications/data-and-digital-ministers-meeting-outcomes/4-november-2022> (Accessed: 11 January 2023).

Department of Finance (2022b) *Data and Digital Ministers Meeting Communique 25 March 2022 | Department of Finance*. Available at: <https://www.finance.gov.au/publications/data-and-digital-ministers-meeting-outcomes/25-march-2022> (Accessed: 11 January 2023).

Grenfell Tower Inquiry (2019) *Grenfell Tower Inquiry: Phase 1 Report (Volume 1)*. House of Commons: London. Available at: <https://assets.grenfelltowerinquiry.org.uk/GTI%20-%20Phase%201%20full%20report%20-%20volume%201.pdf> (Accessed: 8 August 2022).

Fishenden, J. (2014a) ‘20 years of “online government” 101. Part 1: progress towards a single online presence (including pictures)’, new tech observations from the UK (ntouk), 19 March. Available at: <https://ntouk.wordpress.com/2014/03/19/20-years-of-online-government-101-part-1-progress-towards-a-single-online-presence-including-pictures/> (Accessed: 30 April 2019).

Fishenden, J. (2014b) '20 years of "online government" 101. Part 2: "e-government" architectures', new tech observations from the UK (ntouk), 29 March. Available at: <https://ntouk.wordpress.com/2014/03/29/20-years-of-online-government-101-part-2-e-government-architectures/> (Accessed: 30 April 2019).

Fishenden, J. (2014c) '20 years of "online government" 101. Part 3: approaches to identity', new tech observations from the UK (ntouk), 8 April. Available at: <https://ntouk.wordpress.com/2014/04/08/20-years-of-online-government-101-part-3-approaches-to-identity/> (Accessed: 30 April 2019).

Henman, P. (2017). 'The computer says' DEBT': Towards a critical sociology of algorithms and algorithmic governance', Data for Policy. <https://doi.org/10.5281/zenodo.884117>.

Henriques-Gomes, L. (2019) 'Centrelink cancels over 40,000 robodebts, new figures reveal', *The Guardian*, 6 February. Available at: <https://www.theguardian.com/australia-news/2019/feb/06/robodebt-faces-landmark-legal-challenge-over-crude-income-calculations> (Accessed: 28 October 2022).

Henriques- Gomes, L. (2020a) 'Robodebt-related trauma': the victims still paying for Australia's unlawful welfare crackdown', *The Guardian*, 20 November. Available at: <https://www.theguardian.com/australia-news/2020/nov/21/robodebt-related-trauma-the-victims-still-paying-for-australias-unlawful-welfare-crackdown> (Accessed: 8 August 2022).

Henriques-Gomes, L. (2020b) 'Robodebt official challenged by mothers of two young men who took their own lives', *The Guardian*, 17 August. Available at: <https://www.theguardian.com/australia-news/2020/aug/17/robodebt-official-challenged-by-mothers-of-two-young-men-who-took-their-own-lives> (Accessed: 8 August 2022).

Hicks, M. (2017) *Programmed inequality: how Britain discarded women technologists and lost its edge in computing* (1st edition). Cambridge, MA: The MIT Press.

Hillyard, P., Pantazis, C., Tombs, S. and Gordon, D. (eds) (2004) *Beyond criminology: taking harm seriously*. London: Pluto Press.

Hillyard, P. and Tombs, S. (2004) 'Beyond criminology?' in Hillyard, P., Pantazis, C., Tombs, S. and Gordon, D. (eds), *Beyond criminology: taking harm seriously*. London: Pluto Press. pp.10-29.

Human Rights Law Centre (2021) 'The Federal Court approves a \$112 million settlement for the failures of the Robodebt system', 11 June. Available at: <https://www.hrlc.org.au/human-rights-case-summaries/2021/9/30/the-federal-court-approves-a-112-million-settlement-for-the-failures-of-the-robodebt-system> (Accessed: 28 October 2022).

Knaus, C. (2017) 'Almost half of all Centrelink robo-debt cases sent to private debt collectors', *The Guardian*, 11 April. Available at: <https://www.theguardian.com/australia-news/2017/apr/12/almost-half-of-all-centrelink-robo-debt-notices-sent-to-private-debt-collectors> (Accessed: 10 August 2022).

Leigh Day (2022) 'Universal Credit: were you moved to UC before 16.1.19 and lost disability premiums?'. Available at: <https://www.leighday.co.uk/our-services/employment-law-claims-and-disputes/universal-credit-group-action/> (Accessed: 28 October 2022).

Maier-Katkin, D., Mears, D. and Thomas, B. (2009) 'Towards a criminology of crimes against humanity', *Theoretical Criminology*, 13(2), pp. 227-255. <https://doi.org/10.1177/1362480609102880>.

Medhora, S. (2019) Over 2000 people died after receiving Centrelink robo-debt notice, figures reveal, *triple j*, 18 February. Available at: <https://www.abc.net.au/triplej/programs/hack/2030-people-have-died-after-receiving-centrelink-robodebt-notice/10821272> (Accessed: 7 August 2022).

Peachey, K. (2022) 'Post Office scandal: what the Horizon saga is all about', *BBC News*, 22 March. Available at: <https://www.bbc.com/news/business-56718036> (Accessed: 7 August 2022).

Perrow, C. (2011) *Normal accidents: living with high risk technologies (updated)*. Princeton: Princeton University Press.

Rethink Mental Illness (2021) *Tip of the Iceberg? Deaths and serious harm in the benefits system*. July 2021. Available at: <https://www.rethink.org/media/4758/tip-of-the-iceberg.pdf> (Accessed: 26 October 2022).

Schwendinger, H. and Schwendinger, J. (1975) 'Defenders of Order or Guardians of Human Rights' in Taylor, I., Walton, P. and Young, J. (eds) *Critical Criminology*. London: Routledge & Kegan Paul. pp. 113-146.

Thomson, R. (2009) Bankruptcy, prosecution and disrupted livelihoods - Postmasters tell their story, *ComputerWeekly.com*, 11 May. Available at: <https://www.computerweekly.com/news/2240089230/Bankruptcy-prosecution-and-disrupted-livelihoods-Postmasters-tell-their-story> (Accessed: 7 August 2022).

Thorp, L. (2019) '“I've had to report suicides” – Universal Credit worker's harrowing account of benefit's failures', *Liverpool Echo*, 8 December. Available at: <https://www.liverpoolecho.co.uk/news/liverpool-news/ive-report-suicides-universal-credit-17378456> (Accessed: 26/10/2022).

Tombs, S. (2017) 'Grenfell: The unfolding dimensions of social harm', *Justice, power and resistance*, 3(1): 61-88.

Wallis, N. (2022) 'Numbers matter', *Post Office Scandal*, 13 February. Available at: <https://www.postofficescandal.uk/post/numbers-matter> (Accessed: 7 August 2022).

Watt, R. (2017) 'Grenfell Tower fire – a tragic case study in health inequalities', *British Dental Journal*, 223: 478-380. <https://doi.org/10.1038/sj.bdj.2017.785>.

Whiteford, P. (2020) 'Robodebt was a fiasco with a cost we have yet to fully appreciate', *The Conversation*, 16 November. Available at: <https://theconversation.com/robodebt-was-a-fiasco-with-a-cost-we-have-yet-to-fully-appreciate-150169> (Accessed: 28 October 2022).

Witherow, T. and Trump, S. (2021) 'Post Office IT scandal is blamed for FOUR suicides: Grief-stricken relatives are still battling for compensation amid tragic fallout', *Daily Mail*, 27

December. Available at: <https://www.dailymail.co.uk/news/article-10348583/Post-Office-scandal-blamed-FOUR-suicides.html> (Accessed: 28 October 2022).

