

## CHAPTER 2

# Automated Governance: Digital Citizenship in the Age of Algorithmic Cruelty

### Introduction

In March 2020, days after Covid-19 was declared a pandemic by the World Health Organisation (Lupton 2022), and shortly before the UK government announced a full lockdown, all secondary and post-secondary school exams, typically sat at ages 14–16 and 18–19, were cancelled (The Uni Guide n.d.). In their stead, national examination regulatory bodies (Ofqual in England, Qualifications Wales in Wales, Scottish Qualifications Authority in Scotland, and CCEA in Northern Ireland) used an algorithm to calculate students' marks. Ofqual argued that awarding results based solely on teachers' predictions would be misleading and would result in inflated marks, whereas the algorithm produced to determine marks would provide a more accurate picture based on a complex calculation that included not just the individual's records but the student's school's performance overall, at present and in previous years (Burgess 2020). This decision had a substantial impact on many young people as these exam results are central to UK college and university entry criteria and individuals' chances of successfully securing a place at their institution of choice. When results produced by the algorithm were announced in summer 2020 it quickly transpired that, in many cases, students attending better performing schools, which were largely located in wealthier areas, received upgraded marks compared to their teacher's predictions, while students from disadvantaged areas and low resourced schools had their marks downgraded compared to their teacher's predictions and lost out on attending their preferred institutions (Akec 2020).

---

#### How to cite this book chapter:

Kuntsman, A. and Miyake, E. 2022. *Paradoxes of Digital Disengagement: In Search of the Opt-Out Button*. Pp. 41–58. London: University of Westminster Press.  
DOI: <https://doi.org/10.16997/book61.c>. License: CC-BY-NC-ND 4.0

In August, after a wave of protests by young people, objections by teachers and parents/guardians, and a general media storm, Ofqual and the Secretary of State for Education revisited their decision and scrapped the use of what was repeatedly described as a ‘flawed algorithm’ (Akec 2020; Express and Star 2020; Great Yorkshire Radio 2020; Hussain et al. 2020; Smith 2020; Sussex Students’ Union 2020) for England, Wales and Northern Ireland, with Scotland shortly following suit. The decision to deploy algorithms to determine grades came in the middle of a global public health emergency, when many activities had to be cancelled or postponed, and when numerous alternative arrangements had to be quickly conceived, often through a fast-tracked development process, and rushed into implementation. In the case of exams, the hasty nature of these decisions and their immediate and collectively visible impact (hundreds of young people across the country receiving their exam results at the same time, having already been affected by the lockdown and school closures), meant that the deployment of algorithms instead of actual exams received exceptional publicity. Following this collective uproar, the move was relatively easy to undo, especially, one could argue, by the Prime Minister, Boris Johnson, whose handling of the pandemic was generally based on numerous ‘U-turns’ (Rawlinson 2020). In contrast, the use of automated decision-making processes by state bodies in other areas that deal with people’s livelihoods, wellbeing, freedom and survival, has been steadily creeping in and increasing in recent years, in the UK and elsewhere, their strengthening grip less visible, and much harder to challenge.

This chapter examines the growing impossibility of digital refusal or opt-out of algorithmic decision-making and other forms of digitised governance when it comes to the management of civic life, in particular by those most vulnerable to, and/or most dependant on, the state. We begin with a discussion of the UK Government’s ‘digital transformation’ plan. Similar to many other countries’ move to ‘e-government’, the UK plan included moving all public services and their various application processes (visas, welfare, council tax payments etc.) online. It also included communicating with citizens via social media and automating as many decision-making processes as possible, with the help of AI and algorithms. Reading the UK Government’s idealised vision of efficient state services, and happily serviced and digitally engaged citizens, against the grain, this chapter contrasts these narratives of e-government with the realities of growing violence inflicted by digital policing, digital welfare and digital immigration management on those most vulnerable to it, and often most powerless to resist.

We position our discussion within the broader concern of what it means to be a digital citizen – not so much around political behaviour such as voting or activism, nor around citizen participation in civic life at the communal, hyper-local or national level – all of which are more traditional domains of scholarship on digital citizenship (Hintz et al. 2019; Mossberger et al. 2008). Instead, we focus on how interactions between the individual and the state, in areas such as public services, border management and policing, are mediated by digital

platforms, online communication, algorithms and AI. In the field of e-governance/e-government, these new developments have been overwhelmingly welcomed, with much of the work focusing on managerial and institutional efficiency, improvement of public services and citizens' trust, and challenges to development and implementation (Bertrand 2020; European Commission 2020; Reddick 2010; Scholl 2015; Zuiderwijk et al. 2021). Our own analysis is deeply critical of the celebratory approach to e-governance, both due to its solutionist nature, and because it tends to prioritise efficiency over care, and bureaucracy over justice. Instead, we are informed by a growing body of critical scholarship that attends to the relations between digital governance and the rapid expansion of digital state surveillance of the poor and the racialised, the racial and class violence of digital bureaucracy, and the militarisation of digital tools for state xenophobia and racism (Benjamin 2019a; 2019b; Gangadharan 2012; 2017; 2020b; Privacy International 2021; Williams 2018; Williams and Kind 2019).

### The State's New Digital Clothes

In 2012, the UK government introduced its strategy for the digital transformation of government and public services. The strategy, 'set out to how the government will become *digital by default*', (Cabinet Office 2012: emphasis added) and was not dissimilar to many other countries that have that have adopted the e-government model of providing public services through one-stop online platforms, offering 'electronic and mobile services for the benefit of all' (United Nations 2016). The online presence of public services is constantly evolving. At the time of writing in 2021, a series of interlinked pages on the 'gov.uk' website presented the digital transformation strategy as friendly, citizen-facing datafied efficiency, streamlined, service-oriented and empowering:

We will transform the relationship between citizens and the state – putting more power in the hands of citizens and being more responsive to their needs. The tools, techniques, technology and approaches of the internet age give us greater opportunities than ever before to help government:

- better understand what citizens need
- assemble services more quickly and at lower cost
- continuously improve services, based on data and evidence (Cabinet Office 2017).

Set up as 2013–2017 and 2017–2020 strategic plans to move to digital by default by 2020, the policy is centred around the Government Digital Service (GDS), encompassing all public services and 'leading digital transformation' in the

UK (Government Digital Service n.d.). There are several elements to GDS, relevant to the shrinking space of digital disengagement, that are important to mention here.

First and foremost, it is worth noting the kind of citizen/service recipient rendered on the GDS website – a citizen that is not only skilled enough to navigate multiple ‘gov.uk’ webpages, but also proficient in, and comfortable with, the idea of using social media for contacting the authorities. In GDS, the boundary between official ‘gov.uk’ webpages and social media ones is consistently blurred. GDS has a blog and also holds, or has held, accounts on Twitter, Instagram, LinkedIn, YouTube, Flickr and Tumblr. Some of these accounts are more active than others, and some are no longer in use. On most of these social media accounts, at the time of writing in 2021, the engagement ‘metrics’, such as the number of followers, were rather low compared to other organisations or groups using the platforms to communicate with the public. This suggests that, at present, social media is not the primary channel for communication for locating or receiving government information. Nevertheless, it is one that is growing consistently according the GDS website, where the importance of social media engagements is discussed in detail (Government Digital Service 2018b). Currently, GDS does not have a presence on Facebook (explained on their website as due to a lack of resources and the commercialisation of news-feed algorithms which prioritise paid content); Snapchat (explained as due to Instagram being more popular); or TikTok (justified via the demographics of the platform’s users being mostly under 35 and therefore not GDS’s ‘target audience’). These choices and justifications pose not only the question of which groups are prioritised the most, and why – but crucially, which are ignored and abandoned entirely.

Beyond the demographics of ‘engagement’, the social mediatisation of governmental services in itself requires us to pause for a moment. How can we read state power, when its decision-making bodies begin to speak the informal language of platform sociality (van Dijck et al. 2018)? For example, GDS blogs use the vernacular style of social media connectivity, most noticeable when they end their posts by issuing the following invitation: ‘Be a friend, follow us on @GDSteam on Twitter, @GDSteam on Instagram and Government Digital Service on LinkedIn, and engage with our content!’ (Schneider 2020). In the age of the high spread of social media, on the one hand, and corporate platform communication, on the other, such social mediatisation of the state is increasingly blurring the lines between the communal, the corporate and the political.<sup>1</sup> Furthermore, the use of vernacular grammars of ‘being a friend’ (made popular by Facebook) or a follower (used across most platforms) by government services that hold the authority to make decisions fundamental to individual livelihoods and freedom is a powerful, and powerfully masqueraded, tool of state

---

<sup>1</sup> We further discuss the complex relations between social mediatisation and the corporatisation of communication outside leisure and social relations in the next chapter.

rule. At a time when citizens' social media behaviour is increasingly subjected to state surveillance and interrogation, for example by the police (Williams and Kind 2019) or welfare services (Alston and Veen 2019; National Audit Office 2018) one only needs to be reminded that although the platform 'friendship' of liking one's online content is (still) optional, the possibility of 'de-friending' the government online is a dangerous illusion.

All the while, social media surveillance and platform data mining are presented by GDS as the most suitable tools to support and improve public outreach. For example, GDS relies heavily on 'social media listening' (sic) and audience analytics, provided by social media platforms:

Government departments use *different commercial social media listening tools to monitor for specific mentions of words or phrases to learn what people are saying online*. Pricing models vary from product to product, and often depend on the volume of mentions you want to analyse or the number of user accounts you need.

[...]

*Monitoring tools* provide audience insights including demographic data, location and interests.

*Each social media platform has built-in analytics for insights into your audience*. Some will give you more detailed insights that can help you to reach new communities and improve how you communicate with your existing followers (Government Digital Service 2018a).

GDS runs its own social media campaigns and supports various public services to do so too, noting that they 'prefer to measure engagement rather than reach or impressions.' Engagement, here, is of course digital, and is measured through a range of metrics, obtained from Google, social media, and manual analysis (Figure 2.1).

In its Social Media Playbook – a set of guidance on how social media is or can be used in public services – the everydayness of surveillance (monitoring conversations, cross-referencing and analysing multiple types of data, tracking links and drawing on corporate platform analytics etc.) is both laid bare and trivialised, wrapped into the marketing-style language of 'understanding', 'reaching' and 'improving communication'. Becoming 'digital by default' thus traps the user of public services between dependence on the state and its chosen modes of providing services, *and* the datafication of everyday sociality, deeply embedded in corporate platform power and the digital industry.

This datafication and surveillance is both collective *and* individual. It is crucial to remember that digitality-by-default operates through a Janus-faced personalisation. Public services are repeatedly presented as streamlined and easy to use, because they are tailored to individual needs and accessibility requirements and designed to be accessible from all devices and with inclusivity in mind (Allum 2020; Central Digital and Data Office 2021; Service Manual 2016).

### Measure and evaluate your performance

To ensure evaluation relates back to our objectives, we monitor insights continually and feed these back into the campaign - rather than evaluating at the end. We prefer to measure engagement rather than reach or impressions. It's a more tangible way of assessing whether people are consuming our content.

We produce a monthly detailed engagement report for internal stakeholders.

There are various ways to measure an objective has been met, and general data source that can provide the measurements.

Metric	Data source
Number of online mentions across all channels	Social media monitoring tool
Reach of hashtag	Hashtag tracking tool/social media monitoring tool
Impressions generated by content on owned social media platforms	Social media platform's native analytics tools
Social media likes and comments	Social media platform's native analytics tools
Social media shares (including Twitter retweets)	Social media platform's native analytics tools
Video views and subscribers	Social media platform's native analytics tools
Blog subscribers	Blog analytics
Number of users adopting campaign hashtag	Hashtag tracking tool/social monitoring tool
Clicks to website	Google Analytics
Downloads/requests for information	Google Analytics
Number of times owned content has been embedded elsewhere	Social monitoring tool
Sentiment	Social monitoring tool combined with manual analysis using a dip test of responses
User generated content developed outside of owned channels	Social monitoring tool

**Figure 2.1:** ‘Measure and evaluate your performance’, from Social Media Playbook (Governmental Digital Service 2018b).

Personalisation, at the same time, is anchored in digital monitoring and governance of the individual. Beyond platform mining and monetisation of *collective* data, the receipt of governmental services is grounded in a network of *individual* data capture which one cannot opt out of without potentially losing access to the services provided, or without jeopardising ease of access. For example, biometric data, in the form of voice recognition, has already been used for several years by those accessing services for processing tax credits, childcare and other benefits (HM Revenue & Customs 2018). At present, GDS are working on a datafied, biometrically anchored single profile for all government services (Allum 2020). The rewards promised by this new, and ‘constantly improving’, form of e-government, must be assessed against the perils of digital personalisation that may appear as optional, well-regulated and safe, but are de facto extremely limiting of the possibilities of opting out of digital services without a substantial loss of services. At times, as will be shown later in this chapter, such opt-out is not possible at all – and this is where the individual inability to opt out is deeply grounded in collective injustice, targeting the racialised and the poor.

Finally, GDS operates through what can be described, using Ahmed’s words, as a ‘non-performative’ performance of transparency (2012). Non-performativity, for Ahmed, refers to statements that do *not* do what they say – in the context of her work this refers to anti-racist statements by institutions that do not

change their institutional racism. Here, we refer to non-performative transparency, where information appears to be present, while the processes of decision-making remain concealed. On its website, the digital transformation strategy provides detailed information on Design Principles (Central Digital and Data Office n.d.), the Digital Service Standard (Service Manual n.d.) and a Technology Code of Practice (Central Digital and Data Office n.d.) for developing digital public services. Here, the heavy emphasis is on *how* the services are communicated, *how* the messages to the public are framed, or even *how* the service is designed (for example, from an accessibility point of view) rather than on what the public services actually do and how the decision-making process itself works. What we see here is a simultaneous process of overinforming and omitting information. On one hand, the site presents extensive information on technical design standards and principles, which is very important to stakeholders or technical professionals, but is beyond the comprehension (and often, interest) of most ordinary service-users. On the other hand, for users, the 'backstage' of the service itself is explicitly invisibilised through the rationale of making the service 'easy and accessible' (Government Digital Service 2016; Central Digital and Data Office n.d.):

GOV.UK is built on the principle that you *shouldn't need to know* how the government works to use government services. We do the hard work to make things simple for users. That means we make interactions with the government easy, effective and accessible, for example by using language that's familiar to our users instead of complicated legal terms (Allum 2020: emphasis added).

Such concealment is not harmless. As we demonstrate in the next section of this chapter, the technical and procedural blackboxing (Pasquale 2016) of public services processes, and in particular, its architecture of digital tools and its mechanics of decision-making, can make the system impenetrable, and its algorithmic decisions impossible to challenge – all with dire human consequences.

### The State's New Digital Weapons

What, then, is the human cost of e-governance for those on the receiving end of digitisation by default – distress, despair, loss of income, poverty, starvation, imprisonment, death? Who are its captive subjects, its dependant victims? One of the key areas in which digitisation of public services has developed rapidly in the last few years is welfare provision. In 2019, the Guardian published the results of an investigation into the rise of 'digital welfare' around the globe, referring to the use of AI, algorithmic modelling, and prediction, as well as other data systems such as biometrics, in processing, decision-making and management of those most vulnerable in their reliance on state support: child, disability and other benefits; social housing; pensions; and employment and income support



(Pilkington 2019). The Guardian's investigation found that the rapid process of digitisation often worked in tandem with welfare reforms, such as the introduction of 'universal credit' (UC) in the UK<sup>2</sup> a single 'point' system replacing a range of benefits (income support, housing benefits, tax credits etc.), a change which for many resulted in a substantial reduction in the amount received.

The UC reform did not merely change the calculation of which type of support individuals are entitled to, but transformed how welfare is accessed, making the claim process harder, while making the denial or underpayment of benefits easier, 'automating poverty' and 'punishing the poor' (Pilkington 2019). As of the late 2010s, most universal credit applications need to be completed online, despite many of the recipients not being digitally literate, lacking access to a suitable device, or even unable to write (Booth 2019). Beyond issues of digital accessibility, the application process itself is incredibly complicated and obscured, making it practically impossible to understand the process or challenge decisions which are fundamental to one's livelihood, finances and survival. As the Child Poverty Action Group stated in their report, entitled 'Computer Says 'No!':

[t]he information provided via the UC online account (the main way claimants manage their UC claim and communicate with the Department for Work and Pensions (DWP)) does not make it clear that UC is a decision-based system, which has consequences when claimants need to challenge decisions relating to their claim (Howes and Jones 2019).

In digitising welfare services, the Action Group notes, the algorithmic decision-making process is blackboxed not only from recipients but from helpline staff who do not have access to a full calculation of awards and are thus unable to either explain the process or change its outcomes. This lack of transparency is coupled with plentiful evidence on numerous 'errors', some of which are acknowledged by DWP itself (Wall 2019) – errors that are echoed globally, where a glitch in the system, a wrongly ticked box, or even a case of misplaced, lost or mismanaged data, results in distress, loss of welfare support, homelessness, starvation and even death (Howes and Jones 2019; Murphy 2019). However, it would be a mistake to dismiss (or fix) these as merely 'flaws', 'errors', or what Noble (2018, 6) calls 'data aberrations', in an otherwise effective and efficient system. The welfare system itself has a long history of structural racial and classed violence, in the UK and elsewhere (Boushel 2000; Neubeck and Cazenave 2001; Lewis 2000). And now, as several journalists and NGO investigators have powerfully demonstrated, the design of a welfare system that is algorithmically driven *and* digital by default in the ways citizens communicate

---

<sup>2</sup> Although UC is a UK-wide benefit system, it is managed separately in Scotland, via gov.scot rather than the gov.uk site (Scottish Government n.d.).



with the state, is the new face of state cruelty, dressed in the language of efficient public services.

Similar cruelty is at the core of the digitisation of policing. Reminding us that technologies are neither neutral nor merely replicating social injustice, but are racist and discriminatory by design (see also: Benjamin 2019a, 2019b), British criminologist Patrick Williams demonstrates how the digitisation of policing generates biased outcomes, because it is based on fundamentally biased data. In his extensive research of racialised policing in the UK and Europe, Williams notes that the data-driven criminalisation of people of colour, and in particular Black people, is based on the marriage of racist criminalisation such as racialisation of suspicion and being ‘matrixed’ because of skin colour, or being made guilty by association, (Williams 2018) and the ‘encroachment of technology’ (Williams and Kind 2019). The latter refers to an extensive and all-encompassing network of digital identification technologies (mobile fingerprint units, biometrics, automatic number plate recognition, facial recognition, mining of social media content, phone location data), connected to multiple databases and coupled with predictive analytics. Combined together, these technologies are leading to a devastatingly high level of over-policing and over-convicting of Black and other communities of colour, and other forms of short and long term ‘data harms’ of both individuals and communities (Williams and Kind 2019). Williams’ analysis echoes similar scholarship carried out in the US context (Benjamin 2019a, 2019b; Gangadharan 2012, 2020a; Noble 2018), linking long histories of racial and class violence to discrimination and oppression and to what Benjamin poignantly coins ‘carceral technoscience’ (2019a).

An examination of increased digitisation of welfare and policing in the UK shows that digitisation of state-citizen relations is based on a deliberate and complex weaponisation of digital technologies and data embedded into the very heart of e-governance.<sup>3</sup> So what happens to e-governance when it is challenged? What happens in moments of rupture or critique – and thus possible opt out of the digital, as for example, with the case regarding exam results in summer 2020? At around the same time as the exam results furore, the Home

---

<sup>3</sup> Gangadharan makes a similar argument regarding the US context, showing that forced adoption of digital technologies in workplaces, welfare and law enforcement has detrimental impacts on the lives of marginalised and oppressed communities. Her discussion is based on the premise that marginalised groups lack opportunities to advocate for equality because of ‘the shift from public decision making, which affords a measure of transparency, accountability, and democratic legitimacy, to private sectors, which typically lack all three’ (2020a, 128). The UK case demonstrates another angle to this problem, where the seemingly public decision-making processes take place at the intersection of shadow privatisation of governmental IT contracting and public policy that is discriminatory and cruel despite having a democratic legitimacy.

Office was challenged by human rights groups for its use of a racially biased algorithm (McDonald 2020a). For several years, the Home Office – which, tellingly, introduced its ‘hostile environment’ policy around the same time as the launch of governmental ‘digital transformation’ (set in 2012 and implemented from 2013) – was using algorithmic decision-making for processing visa applications.<sup>4</sup> The algorithm was ‘streaming’ applications by nationality, offering ‘speedy boarding’ to applicants from rich, white countries such as the US, Canada, Australia or Western Europe, while ‘poorer people of colour get pushed to the back of the queue’, as noted by the digital rights group Foxglove (Foxglove 2017). Further to the streaming itself, the Foxglove team argued, the ‘algorithm suffered from “feedback loop” problems known to plague many such automated systems – where past bias and discrimination, fed into a computer program, reinforce future bias and discrimination’ (Foxglove 2020). After a set of legal challenges, brought by Foxglove and The Joint Council for the Welfare of Immigrants (JCWI) over several years, the Home Office agreed to scrap the algorithm in 2020 (McDonald 2020b).

The Home Office’s decision was widely celebrated as a victory and an acknowledgement of systemic racism in tech design (BBC News 2020). This was an important milestone in the battle to opt out of biased tech. Yet, just as in the exam results case, ditching one ‘bad’ algorithm can dangerously obscure the systemic violence by design of digital governance of people’s lives, and the marriage of racism, xenophobia and the war on the poor and the disabled with powerful technologies that are integrated in the lives of everyone, but impact everyone differently. As Noble and many others (Benjamin 2019b; Isaac 2018; Kitchin 2021; Lum and Isaac 2016; Williams 2018) remind us, the ‘errors’ we seem to ‘expose’ are never accidental. Rather, they are part of systemic ‘discrimination [that] is [...] embedded in computer code and, increasingly, in artificial intelligence technologies that we are reliant on, by choice or not’ (Noble 2018, 1). When the majority of everyday interactions with the state are digitised, and when such digitisation, in turn, cements the power of discriminatory tech, the disappearing space of opt-out, and the need to reclaim it, becomes central to questions of collective social justice.

### Imagining Alternatives

The rise of digital public services and the overall digitisation of citizen’s lives has also resulted in the rise of critique and resistance. The lead effort among these is the demand for transparency in digital services and processes, by

---

<sup>4</sup> The ‘hostile environment’ – a UK racist policy towards immigration, aimed to make the country inhospitable to migrants, and was presented by the Home Secretary Theresa May in 2012 (Kirkup and Winnett 2012).

organisations supporting specific groups (such as Child Poverty Action Group or JCWI mentioned in this chapter), or by those explicitly focusing on digital rights, such as Foxglove. Frontline journalistic investigations, both in the mainstream media such as the Guardian, and in groups such as The Bureau of Investigative Journalism, are also inquiring into governmental ‘IT contracting’ and the resulting lack of transparency and accountability with regards to public spending (Black and Safak 2019). Indeed, as noted by Pasquale, the call for algorithmic accountability is a growing field of concern for lawyers, journalists, computer and social scientists, and policy makers as well as activists, and that the growing use of algorithms and AI is also leading to new legislation and regulatory frameworks around the auditing and transparency of algorithmic decision-making processes (Pasquale 2019).

However, algorithmic accountability also contains a dangerous paradox. While potentially protecting individuals affected by ‘errors,’ and while making the public more aware of algorithmic involvement in policies and services, improving the work of an algorithm through accountability and auditing processes is a form of digital solutionism, cementing and strengthening digitisation itself. Furthermore, algorithmic transparency itself does not solve the issue of systemic discrimination. As Williams and Kind (2019) remind us, the impact of biometrics, AI and other digital technologies disproportionately affects minority communities in the UK and Europe, who are already over-policed, and now even more so through technologies that are discriminatory by design. These technologies mis-identify Black and other people of colour at a much higher rate, bringing the long history of racism in policing and law enforcement into technology driven geographic and demographic over-criminalisation. A similar analysis is made by contributors to *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life* (Benjamin 2019a), who discuss at length how digital technologies are embedded in carceral regimes in the US and globally. Long-standing histories of harm, erasure and oppression are not merely receiving a new incarnation through discriminatory tech. Rather, as Benjamin argues, racist and classist social control explicitly propels investment in discriminatory designs.

Moving beyond algorithmic transparency, Pasquale suggests that we need to move towards a second wave of algorithmic accountability: ‘while the first wave of algorithmic accountability focuses on improving existing systems, a second wave of research has asked *whether they should be used at all—and, if so, who gets to govern them*’ (2019: emphasis added). Following Pasquale, we propose to expand this formulation to the notion of *digital accountability*, where digital disengagement is precisely the paradigm for asking questions such as, do we need this particular technology/device/app/tool to begin with, and if we do, where would a way out be? Furthermore, digital accountability must not merely take systemic injustice into account but use it as its starting point in the abolition of racist tech (Benjamin 2019a, 2019b; Williams 2018) and of ‘digital technologies that punish and police marginalised people’ (Gangadharan

2020a). As Williams poignantly notes, opposing racist digital policing, and racist tech more broadly, cannot stem merely from opposition to surveillance and infringements on privacy, but must be embedded in an anti-racist and justice-oriented approach. In a similar vein, Benjamin calls for the abolition of all carcerality (2019a). Finally, Gangadharan (2020a) emphasises that digital refusal and collective civil disobedience against technological coercion must centre the experiences of marginalised communities. Such an approach, while systemic in its orientation, also, crucially, comes from below, and leads us to the other alternative to digital encroachment of the state, with which we conclude this chapter.

The second alternative is digital self-defence – a broad term that describes a range of mostly grassroots, bottom-up initiatives to protect individuals and communities from digital surveillance and tracking. The logic of digital self-defence is starkly different from that of cybersecurity – even though both focus on safety and protection in the digital world. The militarised logic of cybersecurity usually involves centralised control (state and/or corporate), hierarchical power, authorised expertise and often also invokes a sentiment of war – ‘us vs them’, ‘rules of combat’, and other frameworks that centre and justify violence and suppression, while assigning legitimacy to structural powers. Digital self-defence, on the other hand, prioritises empowerment, non-hierarchical knowledge and protection of those vulnerable to state and/or corporate power. Examples of digital self-defence are countless, and can include NGOs and community-oriented projects such as ‘Our Digital Bodies’ (ODB 2016), a collective based in marginalised neighbourhoods in the US that tackles digital data collection and human rights and fosters individual and community-based forms of digital refusal (Benjamin 2019b; Gangadharan 2020b, 2020c), or ‘RosKomSvoboda’ (Роскомсвобода 2014) – a Russian NGO supporting internet self-regulation, digital rights and freedom from state censorship (the name literally meaning ‘Russian Communication Freedom’, a paraphrasing of RosKomNadzor, the name of Russia’s ‘Federal Service for Supervision of Communications, Information Technology and Mass Media’) (Роскомнадзор n.d.) Digital self-defence also encompasses individual practices such as make-up that helps evade facial recognition systems; advice and guidelines to avoid data aggregation by withholding personal information or obscuring algorithmic analytics (for example, via ‘algorithmic jamming’ (Wood 2020)) and deliberately erratic search behaviour; protecting one’s identity via fake digital profiling (Heuer and Tranberg 2013) as well as community-based technical education around encryption; and hacktivism.

### **Conclusion: From Digital Violence to Digital Self-Defence**

Informed and inspired by the growing body of scholarship on the militarisation of digital tools for state xenophobia, racism and the war on poor, this chapter took this discussion further by framing the debate on the digitisation of injustice

and algorithmic violence through the question of digital disengagement. The chapter was driven by the following question: what are the possibilities of opting out of digitisation of civic life, who are they afforded to (if at all), and at what cost? Throughout the chapter, we have pointed out that the spaces of civic digital disengagement – access to non-digital public services, or the right to not be subjected to algorithmically managed decisions – are profoundly shaped by social inequalities and are rapidly shrinking. By looking at examples of welfare, policing and border control, we argued that it is imperative to account for the growth of algorithmic violence when digital technologies are adopted within all spheres of everyday life, while having a very different impact on individuals, depending on one's privilege or marginality. We ended this chapter with a discussion of alternatives to current digital governance that are not about merely allowing individual opt-out, but centre equality and collective justice. These included frameworks for transparency and accountability on both legal and technical levels, as well as digital self-defence in the form of bottom-up organising to empower those most vulnerable to the forces of digitisation and algorithmic cruelty.

Ironically, digital self-defence is premised on the advancement of digital literacy. However, unlike digital solutionism which we address in Part II of the book, digital self-defence creates empowerment in contexts where opportunities to opt out are shrinking, but without rendering the tech as necessarily desirable. Digital disengagement, here, is not about disconnecting from online communication or devices in order to take a break or improve one's well-being. Rather, it is a nuanced and focused toolkit for combatting digital violence and digital coercion in their own territory and with their own tools (or with a remake thereof). In doing so, one might disengage from certain expected practices of digital citizenship such as voluntary submission of personal and other information; knowing or unwitting contribution to databases; or compliance with other forms of technologically enhanced structural violence. The actual practices of digital self-defence might range from simply being aware and careful, to actual electronic/digital civil disobedience (Benjamin 2019b; Critical Art Ensemble 2001), to 'reimagin[ing] technoscience for liberatory ends' (Benjamin 2019a, 13), depending on context, country, one's position of marginalisation, and of course, the technology used. What is crucial here is that digital disengagement undoes and disrupts the logic of digital power by navigating the digital field itself.

## Bibliography

- Ahmed, Sara. 2012. *On Being Included: Racism and Diversity in Institutional Life*. Durham: Duke University Press. <https://doi.org/10.1215/9780822395324>
- Akec, Athian. 2020. 'The A-Level Algorithm Chaos Reveals Society's Racist, Classist Biases'. *DazedDigital*, 17 August. <https://www.dazeddigital.com/politics/article/50152/1/a-level-algorithm-grades-chaos-reveals-society-government-racist-social-biases>

- Allum, Jen. 2020. 'Introducing GOV.UK Accounts.' *Government Digital Service* (blog), 22 September. <https://gds.blog.gov.uk/2020/09/22/introducing-gov-uk-accounts/>
- Alston, Philip, and Christiaan van Veen. 2019. 'How Britain's Welfare State Has Been Taken over by Shadowy Tech Consultants.' *The Guardian*, 27 June. <https://www.theguardian.com/commentisfree/2019/jun/27/britain-welfare-state-shadowy-tech-consultants-universal-credit>
- BBC News. 2020. 'Home Office Drops "Racist" Algorithm from Visa Decisions.' *BBC News*, 4 August. <https://www.bbc.co.uk/news/technology-53650758>
- Benjamin, Ruha. (Ed.). 2019a. *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*. Durham: Duke University Press.
- Benjamin, Ruha. 2019b. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity.
- Bertrand, Arnould. 2020. 'Why AI and the Public Sector Are a Winning Formula.' *EY*, 21 October. [https://www.ey.com/en\\_gl/government-public-sector/why-ai-and-the-public-sector-are-a-winning-formula](https://www.ey.com/en_gl/government-public-sector/why-ai-and-the-public-sector-are-a-winning-formula)
- Black, Crofton, and Cansu Safak. 2019. 'How Is Government Using Big Data? The Bureau Wants to Find Out.' *The Bureau of Investigative Journalism*, 8 May. <https://www.thebureauinvestigates.com/stories/2019-05-08/algorithms-government-it-systems>
- Booth, Robert. 2019. 'Computer Says No: The People Trapped in Universal Credit's "Black Hole".' *The Guardian*, 14 October. <https://www.theguardian.com/society/2019/oct/14/computer-says-no-the-people-trapped-in-universal-credits-black-hole>
- Boushel, M. 2000. 'What Kind of People Are We? "Race", Anti-Racism and Social Welfare Research.' *British Journal of Social Work*, 30 (1): 71–89. <https://doi.org/10.1093/bjsw/30.1.71>
- Burgess, Matt. 2020. 'The Lessons We All Must Learn from the A-Levels Algorithm Debacle.' *Wired*, 20 August. <https://www.wired.co.uk/article/gcse-results-alevels-algorithm-explained>
- Cabinet Office. 2012. 'Government Digital Strategy'. Policy Paper. UK Government. <https://www.gov.uk/government/publications/government-digital-strategy>
- Cabinet Office. 2017. 'Government Transformation Strategy'. Policy Paper. UK Government. <https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy>
- Central Digital and Data Office. n.d. 'Government Design Principles: Do the Hard Work to Make It Simple'. GOV.UK. <https://www.gov.uk/guidance/government-design-principles>
- Central Digital and Data Office. n.d. 'Technology Code of Practice'. GOV.UK. <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- Critical Art Ensemble. 2001. *Digital Resistance: Explorations in Tactical Media*. New York: Autonomedia.

- European Commission. Joint Research Centre. 2020. 'AI Watch, Artificial Intelligence in Public Services: Overview of the Use and Impact of AI in Public Services in the EU'. LU: Publications Office. <https://data.europa.eu/doi/10.2760/039619>
- Express and Star. 2020. 'Ofqual's Algorithm "Unfairly Favours Niche Subjects Such as Latin"'. *Express and Star*, 16 August. <https://www.expressandstar.com/news/uk-news/2020/08/16/ofquals-algorithm-unfairly-favours-niche-subjects-such-as-latin/>
- Foxglove. 2017. 'Legal Action to Challenge Home Office Use of Secret Algorithm to Assess Visa Applications'. Foxglove, 29 October. <https://www.foxglove.org.uk/news/legal-challenge-home-office-secret-algorithm-visas>
- Foxglove. 2020. 'Home Office Says It Will Abandon Its Racist Visa Algorithm – After We Sued Them'. Foxglove, 4 August. <https://www.foxglove.org.uk/news/home-office-says-it-will-abandon-its-racist-visa-algorithm-nbsp-after-we-sued-them>
- Gangadharan, Seeta Peña. 2012. 'Digital Inclusion and Data Profiling'. *First Monday*, 17 (5). <https://doi.org/10.5210/fm.v17i5.3821>
- Gangadharan, Seeta Peña. 2017. 'The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users'. *New Media & Society*, 19 (4): 597–615. <https://doi.org/10.1177/1461444815614053>
- Gangadharan, Seeta Peña. 2020a. 'Digital Exclusion: A Politics of Refusal'. In Lucy Bernholz, Hélène Landemore, and Rob Reich (Eds.). *Digital Technology and Democratic Theory*. Chicago: University of Chicago Press.
- Gangadharan, Seeta Peña. 2020b. 'Life and Death: Optimization, Democracy, and Justice'. In AoIR2020 Online. [https://aoir.org/aoir2020/aoir2020keynote\\_plenary/](https://aoir.org/aoir2020/aoir2020keynote_plenary/)
- Gangadharan, Seeta Peña. 2020c. 'Context, Research, Refusal: Perspectives on Abstract Problem-Solving'. *ODBProject* (blog), 30 April. <https://www.odbpject.org/2020/04/30/context-research-refusal-perspectives-on-abstract-problem-solving/>
- Government Digital Service. 2016. 'Content Design: Planning, Writing and Managing Content'. GOV.UK. <https://www.gov.uk/guidance/content-design/writing-for-gov-uk>
- Government Digital Service. 2018a. 'Social Media Playbook'. GOV.UK. <https://www.gov.uk/guidance/social-media-playbook>
- Government Digital Service. 2018b. 'Measure and Evaluate Your Performance'. GOV.UK. 17 August. <https://www.gov.uk/guidance/social-media-playbook#measure-and-evaluate-your-performance>
- Government Digital Service. n.d. 'Homepage'. GOV.UK. <https://www.gov.uk/government/organisations/government-digital-service>
- Government Digital Service. n.d. GDS Team LinkedIn. Instagram. <https://www.linkedin.com/company/2365518/admin/>



- Government Digital Service. n.d. @GDSTeam. Twitter. <https://twitter.com/GDSTeam>
- Government Digital Service. n.d. @GDSTeam. Instagram. <https://www.instagram.com/gdsteam/>
- Great Yorkshire Radio. 2020. 'A-Levels: Ditch "flawed" Algorithm Used for Results, Government Told'. *Great Yorkshire Radio*, 14 August. <https://great.yorkshireradio.co.uk/news/uk/item/5989-a-levels-ditch-flawed-algorithm-used-for-results-government-told>
- Heuer, Steffan, and Pernille Tranberg. 2013. *Fake It!: Your Guide to Digital Self-Defence*. 2nd edition. Scotts Valley: CreateSpace Independent Publishing Platform.
- Hintz, Arne, Lina Dencik, and Karin Wahl-Jorgensen. 2019. *Digital Citizenship in a Datafied Society*. Cambridge: Polity.
- HM Revenue & Customs. 2018. 'Voice Identification Privacy Notice'. GOV.UK. 27 July. <https://www.gov.uk/government/publications/voice-identification-privacy-notice/voice-identification-privacy-notice>
- Howes, Sophie, and Kelly-Marie Jones. 2019. 'Computer Says "No!" – Stage One: Information Provision'. Information Provision. Child Poverty Action Group. <https://cpag.org.uk/policy-and-campaigns/report/computer-says-no-stage-one-information-provision>
- Hussain, Danyal, Jack Maidment, and David Wilcock. 2020. 'Boris Heads on Holiday amid A-Levels Chaos: PM Skips off to Scotland but is "Poised to U-Turn TODAY" on Exams "Shambles" amid Huge Tory Revolt – but No10 Insists GCSE Results WON'T Be Delayed'. *Daily Mail*, 17 August. <https://www.dailymail.co.uk/news/article-8634321/Ofqual-board-members-want-ditch-level-algorithm.html>
- Isaac, William. 2018. 'Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice'. *Ohio State Journal of Criminal Law*, 15 (2): 543–58.
- Kirkup, James, and Robert Winnett. 2012. 'Theresa May Interview: "We're Going to Give Illegal Migrants a Really Hostile Reception"'. *The Telegraph*, 25 May. <https://www.telegraph.co.uk/news/0/theresa-may-interview-going-give-illegal-migrants-really-hostile/>
- Kitchin, Rob. 2021. *Data Lives: How Data Are Made and Shape Our World*. Bristol: Bristol University Press.
- Lewis, Gail. 2000. *'Race', Gender, Social Welfare: Encounters in a Postcolonial Society*. Cambridge: Polity.
- Lum, Kristian, and William Isaac. 2016. 'To Predict and Serve?' *Significance*, 13 (5): 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>
- Lupton, Deborah. 2022. *Covid Societies: Theorising the Coronavirus*. Abingdon: Routledge.
- McDonald, Henry. 2020a. 'Home Office to Face Legal Challenge over "Digital Hostile Environment"'. *The Guardian*, 18 June. <https://www.theguardian.com/uk-news/2020/jun/18/home-office-legal-challenge-digital-hostile-environment>

- McDonald, Henry. 2020b. 'Home Office to Scrap "Racist Algorithm" for UK Visa Applicants'. *The Guardian*, 4 August. <https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants>
- Mossberger, Karen, Caroline J. Tolbert, and Ramona S. McNeal. 2008. *Digital Citizenship the Internet, Society, and Participation*. Cambridge: MIT Press. <https://doi.org/10.7551/mitpress/7428.001.0001>
- Murphy, Katharine. 2019. 'Robodebt Class Action: Shorten Unveils "David and Goliath" Legal Battle into Centre Link Scheme'. *The Guardian*, 17 September. <https://www.theguardian.com/australia-news/2019/sep/17/robodebt-class-action-shorten-unveils-david-and-goliath-legal-battle-into-centrelink-scheme>
- National Audit Office. 2018. 'Rolling Out Universal Credit. Audit. Department for Work & Pensions'. <https://www.nao.org.uk/report/rolling-out-universal-credit/>
- Neubeck, Kenneth J., and Noel A. Cazenave. 2001. *Welfare Racism: Playing the Race Card Against America's Poor*. New York: Routledge.
- Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
- ODB. 2016. Our Data Bodies. OBD Project. 2016. <https://www.odbproject.org/>
- Pasquale, Frank. 2016. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.
- Pasquale, Frank. 2019. The Second Wave of Algorithmic Accountability. *LPE Project* (blog), 25 November. <https://lpeproject.org/blog/the-second-wave-of-algorithmic-accountability/>
- Pilkington, Ed. 2019. 'Digital Dystopia: How Algorithms Punish the Poor'. *The Guardian*, 14 October. <https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor>
- Privacy International. 2021. 'The UK's Privatised Migration Surveillance Regime: A Rough Guide for Civil Society'. Privacy international. [https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK\\_Migration\\_Surveillance\\_Regime.pdf](https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf)
- Rawlinson, Kevin. 2020. 'Boris Johnson's Year of U-Turns: From Covid Tests to Free School Meals'. *The Guardian*, 10 December. <https://www.theguardian.com/uk-news/2020/dec/10/boris-johnson-year-of-u-turns>
- Reddick, Christopher G. (Ed.). 2010. *Comparative E-Government*. New York: Springer.
- Scholl, Hans J. 2015. *E-Government: Information, Technology, and Transformation*. Abingdon: Routledge.
- Schneider, Vanessa. 2020. 'As Social Media Changes, so Does GDS's Playbook'. *Government Digital Service* (blog), 21 September. <https://gds.blog.gov.uk/2020/09/21/as-social-media-changes-so-does-gdss-playbook/>
- Scottish Government. n.d. *Policy/Social Security/Universal Credit*. <https://www.gov.scot/policies/social-security/universal-credit/>
- Service Manual. 2016. 'Designing for Different Browsers and Devices'. GOV. UK. 23 May. <https://www.gov.uk/service-manual/technology/designing-for-different-browsers-and-devices>

- Service Manual. n.d. 'Service Standard'. GOV.UK. <https://www.gov.uk/service-manual/service-standard>
- Smith, Naomi. 2020. 'GCSE Students Narrowly Avoided Ofqual's Flawed Algorithm – But They Won't Escape the Fallout from a Bad EU Trade Deal'. *The Independent*, 20 August. <https://www.independent.co.uk/voices/gcse-results-day-williamson-employment-brexit-eu-trade-a9677726.html>
- Sussex Students' Union. 2020. 'Our Statement on A-Level Results'. *Sussex Student*, 14 August. <https://sussexstudent.com/news/article/statement-alevel-grades>
- The Uni Guide. n.d. 'GCSE Choices and University'. <https://www.theuniguide.co.uk/advice/gcse-choices-university>.
- United Nations. 2016. 'UN E-Government Survey 2016. Survey'. United Nations. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>
- van Dijck, José, Thomas Poell, and Martijn de Waal. 2018. *The Platform Society*. New York: Oxford University Press.
- Wall, Tom. 2019. "I'm 57 and My Parents Have to Feed Me": The Universal Credit Digital Obstacle Course'. *The Guardian*, 18 March. <https://www.theguardian.com/society/2019/mar/18/57-parents-feed-me-universal-credit-digital-obstacle-course>
- Williams, Patrick. 2018. 'Being Matrixed: The (Over)Policing of Gang Suspects in London'. *Stop Watch: Research and Action for Fair and Inclusive Policing*. <https://www.stop-watch.org/our-work/gangs-matrix>
- Williams, Patrick, and Eric Kind. 2019. 'Data-Driven Policing: The Hard Wiring of Discriminatory Policing Practices Across Europe'. European Network Against Racism. <https://www.enar-eu.org/Reports-Toolkits-153>
- Wood, Rachel. 2020. "'What I'm Not Gonna Buy': Algorithmic Culture Jamming and Anti-Consumer Politics on YouTube'. *New Media & Society*, 23 (9): 2754–2772. <https://doi.org/10.1177/1461444820939446>
- Zuiderwijk, Anneke, Yu-Che Chen, and Fadi Salem. 2021. 'Implications of the Use of Artificial Intelligence in Public Governance: A Systematic Literature Review and a Research Agenda'. *Government Information Quarterly*, 38 (3). <https://doi.org/10.1016/j.giq.2021.101577>
- Роскомнадзор (Roskomnadzor). n.d. Роскомнадзор (Roskomnadzor). Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Federal Service for Supervision of Communications, Information Technology and Mass Media). <https://rkn.gov.ru/>
- Роскомсвобода (Roskomsvoboda). 2014. Роскомсвобода (Roskomsvoboda). Roskomsvoboda. <https://roskomsvoboda.org/>