A Liberal Political Philosophy of British Digital Identity Systems

Supervisors: Professors Victoria Nash and Helen Margetts

93,184 words (excl. bibliography)

OXFORD INTERNET INSTITUTE
UNIVERSITY OF OXFORD

Charlie Harry Smith
Balliol College

A thesis submitted for the degree of

Doctor of Philosophy in Information, Communication, and the Social Sciences

Michaelmas Term MMXXIV

Figure 1. A flyer distributed on the 18th of February 2023, at a protest in Oxford.

Table of Contents

Abstract

This thesis evaluates the British state's national digital identity systems using the tools of liberal political philosophy for the first time. Such systems are becoming ubiquitous, with public and private institutions alike looking to embrace people via computerised methods. We are increasingly asked to digitally prove who we are, confirm our age, and authorise transactions by all manner of services. Especially when interacting with government, these tools are rapidly replacing the analogue systems that civil servants have traditionally relied upon to 'know' citizens. Yet the transition has not been easy. Over the past twenty-five years, successive British governments have twice now rolled-out expensive, national systems—each underpinned by a different digital identity architecture—only to see their attempts fail. Nevertheless, the incoming Labour government looks set on deploying a recombinant take on what has come before. If they are to be successful, and avoid the mistakes of the past, lessons therefore remain to be learnt.

Political philosophy has much to say here. But while other disciplines have contributed to the discourse, philosophers have neglected to take note of digital identity systems. This is despite the fact that they raise normative issues of interest to any theorist: questions of freedom and control, access and inclusion, surveillance and privacy. Addressing this oversight, using an empirically-informed version of the method of reflective equilibrium, I construct a novel, liberal-democratic rationalisation of contemporary British digital identity policy. Drawing on fifty-one qualitative interviews conducted with a range of public and private sector stakeholders, I analyse the deeply normative reasons for Britain's uniquely troubled history with identification systems. I then deploy this analysis to generate a coherent policy position, resolving a series of interlinked normative dilemmas: unchecked central oversight, persistent exclusion, and neoliberal economisation. The result should interest theorists, identity experts, and policymakers alike.

Acknowledgements

With the benefit of hindsight, some detours in my doctoral journey—like the coronavirus outbreak or joining the civil service—have been markedly less predictable than others. Yet a whole host of wonderful people have helped ensure that all those twists and turns never seemed unmanageable. Above all, I am deeply indebted to my supervisors, Professors Victoria Nash and Helen Margetts, for all their time, support, and insight over the past five years. Neither has ever given me reason to doubt that the intersection of political philosophy and digital identity was worth exploring, and both have improved my writing and thinking endlessly. Vicki, especially, has shepherded me all the way from eager applicant, phoning for advice from outside the John Radcliffe, to where I stand now, on the eve of the viva.

For half a decade, Oxford has been the academic home I always dreamed it would be. Thank you to all the academics, administrators, and staff at the OII and Balliol for creating such an inspiring environment, amongst such beautiful buildings. From the outset, I must also recognise that it was only due to generous funding from the Economic and Social Research Council's *Grand Union* Doctoral Training Partnership that I have been lucky enough to experience everything the DPhil has to offer. Grand Union funding and support has allowed me to learn far beyond Oxford and its libraries—from Demos, in Whitehall, to Identiverse, in Las Vegas.

My professional life has also gradually become intertwined with my research. I have learnt so much from the identity community. My sincerest thanks must go to my research participants for entertaining questions and occasionally-wild hypotheticals far beyond the remits of their day jobs. Above all, I am most grateful to Nick Mothershaw, Frank Joshi, Jon Nash, Gilad Rosner, Don Thibeau, and Alex Blandford for their expertise and mentorship. More generally, the whole team at the Open Identity Exchange always made industry feel welcoming, while winning the OpenID Foundation's Kim Cameron Award in 2023 was a particular honour. In the past year, however, colleagues at DSIT have shown me a different side of identity. I will forever be glad that Ophelia King, Tom Oldfield, and Hannah Rutter saw value in a political philosophy doctorate. Thank you, too, to Victoria Baines, Georgina Wheatley, and the rest of the Office for Digital Identities and Attributes for bearing with my bifurcated life. All of you have contributed to this thesis in numerous ways. That said, all views—and especially mistakes—in this thesis are mine and mine alone. They do not constitute statements of government policy, and any inferences or assessments represent only my personal views, except where otherwise indicated.

Now, for the personal ones. I must salute my friends and fellow doctoral students from the OII and Balliol; Jakob Schram, Jaimie Lee Freeman, Nayana Prakash, Liam Bekirsky, Thomas Evans, Amanda Curtis, Prathm Juneja, Felix Simon, Laura Herman, Clementine Collett, Hannah Kirk, Joanna Rivera-Carlisle, and Nathan Davies. You all

mean the world to me. At Oxford, Dr Keegan McBride and Professor Jo Wolff have always shown me huge generosity, while the Sirens kept me sane in the early years. Beyond Oxford, my LSE compatriots Zane Jennings and David Rischel remain excellent interlocutors, while Professor Edgar Whitley helped kindle my fledgling interest in identity. But my deepest appreciation must, of course, go to B3, who have supported me for over a decade now. Solomon Lawes, Maya Moss, Thomas Walshe, and the rest of the Britannia crew, you are the best friends I could wish for.

I owe special thanks to my whole extended family, particularly Christopher, Irene, and Richard. But it goes without saying that I am most grateful to my dear parents, Lesley and Russell, and wonderful sister, Gabrielle. Beyond Lesley's invaluable final-week edits, I am so lucky to have benefited from all your unwavering support and encouragement to pursue endless further education—despite occasional worries that I might never be gainfully employed. You have shown me the world, made me who I am, and always been there for me. Thank you for believing in me, and the value of this degree. I have never forgotten how lucky I am to have you all in my life.

Lastly, Laurel Boxall. Every day, you make my world brighter, richer, and happier; and I like to think we have already made a little mark together on the digital state. I could not have done this without you. Above all, thank you for reminding me that the very best bits of life exist outside of work, and for tolerating many a truncated weekend since we decided to take a chance on living together in London. Your endless love, patience, and affection mean everything to me—not to mention all the proofreading and sound-boarding. Here is to some normalcy, at least for a moment, and our next adventure, wherever it takes us. You already know I want nothing more than to share our lives with one another; and, one day soon, to also share a surname.

Canonbury, London
September 19th, 2024

List of Figures

List of Tables

Abbreviations

ATM: *Automatic Teller Machine*

DEG: *Digital Era Governance*

DCMS: *Department for Digital, Culture, Media and Sport*[1]

DfE: *Department for Education*

DSIT: *Department for Science, Innovation and Technology*

DVLA: *Driver and Vehicle Licensing Agency*

EFF: *Electronic Frontier Foundation*

eGovernment: *Electronic Government*

GDS: *Government Digital Service*

HO: *Home Office*

HMG: *His/Her Majesty's Government*

IAM: *Identity and Access Management*

[1] As discussed in Chapter 7, responsibility for 'digital' moved from DCMS to DSIT in 2023 in a machinery of government change instigated by Rishi Sunak's Conservative government.

IdP: *Identity Provider*

LoA: *Level of Assurance*

LSE: *The London School of Economics and Political Science*

MFA: *Multi-Factor Authentication*

MVP: *Minimum Viable Product*

NINO: *National Insurance Number*

NIR: *National Identity Register*

NPM: *New Public Management*

NR: *National Registration*

OLIPAG: *One Login Inclusion and Privacy Advisory Group*

PCAG: *Privacy and Consumer Advisory Group*

PIN: *Personal Identification Number*

RE: *Reflective Equilibrium*

RP: *Relying Party*

SSO: *Single Sign-On*

ULN: *Unique Learner Number*

Chapter 1.

Introduction

"In the twenty-first century, *the digital is political*"

– Jamie Susskind (2020)

On the 18th of February 2023, while crossing Magdalen Bridge, I unexpectedly found myself in the midst of a public protest. Standing aside, a friend and I watched as a heavy police presence escorted the crowd of protestors across the bridge and out of Oxford's city centre. Many held flags and banners, shouted through megaphones, or handed out pamphlets. One such leaflet (Fig. 1) was thrust into my hands. With surprise, I looked down to see my research topic plastered across the page. At the same time, I realised protestors were voicing concerns about the lack of political consent for these new systems, their plummeting trust in government, and the freedoms citizens would lose if they failed to act (Wilcox, 2023). One voice, amplified by a bullhorn, claimed free movement through the streets of Oxford would soon be curtailed; that, without the right digital credentials, people would be prevented from travelling between neighbourhoods. I was ecstatic. Right in front of me, people were associating the systems I researched with some of the most important political concepts and values we hold dear in liberal societies. I promptly took the photo that would become this project's frontispiece and turned, grinning, to my friend. For the first time in my adult life, digital identification felt like a 'live' political issue. What follows—a liberal-democratic rationalisation of Britain's national digital identity policy—can accordingly be read, in part, as a response to what I witnessed that day.

1.1 Identification, Citizens, and the State

In some ways, the protestors were not wrong. Today, digital identity systems do increasingly define us in the eyes of the state (Aaron Martin & Taylor, 2020). They enable governments around the world to recognise and authenticate people during online and offline interactions, granting citizens and residents alike existence in terms that computerised bureaucracies can understand (Sullivan, 2011, p. 9). In doing so, these systems build on practices that far pre-date computers. Since the invention of

paper, identity records have, after all, allowed states to control people (Groebner, 2007); recording who is 'in' and who is 'out', what they deserve, and, above all, who they are. In many countries, such documents even became the sole means by which people could make formal and legal identity claims, conditioning their access to freedoms and resources in the process. Just think of the calls for 'papers, please!' that accompany international border crossings. But, if the digitalisation of identification is a global phenomenon, then why focus on Britain?

Beyond my personal familiarity with the country, Britain's history with such technologies is unusually contested. Unlike most of our European neighbours, who have long-tolerated national identity cards and centralised registers, Britons have repeatedly rejected such solutions (Higgs, 2011), leaving the state to instead develop a patchwork of localised replacements (Higgs, 2004). This makes the country somewhat of an outlier—and an interesting case for exploring the development of alternative approaches.

Indeed, in terms of state identification, we do not need to look too far back in time to find a Britain that would be almost unrecognisable from a modern vantage point. Hard as it may be to believe, on the eve of the First World War the average citizen would have lived an essentially anonymous life, at least in the eyes of the national bureaucracy. Government mostly left people alone and knew very little about them. As historian A. J. P. Taylor (1965, p. 1) has summarised:

> Until August 1914 a sensible, law-abiding Englishman could pass through life and hardly notice the existence of the state, beyond the post office and the policeman. He could live where he liked and as he liked. He had no official number or identity card. He could travel abroad or leave his country for ever without a passport or any sort of official permission. He could exchange his money for any other currency without restriction or limit. He could buy goods from any country in the world on the same terms as he bought goods at home. For that matter, a foreigner could spend his life in this country without permit and without informing the police. Unlike the countries of the European continent, the state did not require its citizens to perform military service. […] broadly speaking, the state acted only to help those who could not help themselves. It left the adult citizen alone.

Nevertheless, the British state has since forged strong links between identification and citizenship. What is more, digital technologies are now becoming central to the transformation. Each year, government collects, processes, and stores vast amounts of information about each and every one of us (Barry, 2020). Today, the average Briton is consequently tied to multiple unique identification numbers, distributed across many different government departments (Glick, 2021d). And, without these systems, the fine-grained interventions that characterise modern policymaking would likely be impossible. Identity systems are vital for distributing state support, securing the borders, and collecting taxes. However, the British government does not monopolise the means of identification. Similar systems condition our relationships in the private sector, too. Corporations are likewise capturing, recording, and analysing more

information about us than ever before[2] (West, 2019). For some, identification is their primary business—a service they provide to other companies, or even back to the government (Higgs, 2013). In the twenty-first century, we therefore regularly prove that 'we are who we say we are' with passwords, personal identification numbers (PINs), face scans, and digital credentials, across both the public and private sectors.

These faster, more precise, and more powerful digital systems are changing the status quo, upending decades of thinking about how, when and where people can and should be identified. Many organisations can now remotely identify and authenticate individuals with little more than a smartphone and access to the internet—displacing the hardcopy document checks and physical human contact that previously defined our interactions (Lyon, 2002). More generally, data and code structure significant aspects of our daily lives (Lessig, 1999, 2006). The changes for citizens and their relationships with important institutions are accordingly stacking up. On the one hand, such systems can contribute towards a more secure, efficient, and effective public sector (CJ Bennett & Lyon, 2008, p. 5). But, on the other, critics are keen to stress that identification systems can be used to "discriminate, infringe [upon] civil liberties and contribute to the spread of surveillance" (CJ Bennett & Lyon, 2008, p. xii). At a time when we may soon need to prove our identities to browse much of the internet (ARTICLE 19, 2022)—and must already present adequate identification to vote, buy or rent a house, and get a job (DSIT, 2024b)—such systems accordingly raise difficult political questions. The protestors, in other words, may have been onto something; there are important trade-offs here that need careful consideration.

1.2 The Contemporary Debate and its Limitations

As the foregoing shows, a deep and uncomfortable tension—perhaps the central tension of digital identity systems—runs through the identity debate, as well as this thesis. For one, powerful, computerised systems can easily place citizens at risk of unwarranted oversight, control, and exclusion. The British state has, for much of its history, effectively used the analogue precursors of such systems for precisely these ends—especially across the Empire (Macdonald & Lenihan, 2018; Sengoopta, 2004). But, at the same time, they can also be deeply positive. Gaining recognition via state identification systems can convey judgements of equality as well as of moral and political worth that open the door to fuller enjoyment of liberty. This is particularly true in a country like Britain, that maintains a welfare state to distribute the goods of citizenship (Iversen, 2021).

Figuring out precisely how to weigh up all these various political and ethical considerations is, therefore, one of the key policy dilemmas surrounding the deployment of such systems today. And finding a resolution is not easy. For twenty-

[2] Banks, credit agencies, and data brokers all maintain particularly powerful, interconnected infrastructures for identifying individuals (Reviglio, 2022).

five years, politicians of all stripes in Britain have struggled to arrive at an acceptable solution. Different governments have repeatedly changed tack, with multiple, sweeping overhauls leaving expensive failures in their wake. Even today, in a country full of divergent stakeholders—not to mention the ever-evolving international context—everything from the technical architecture of such systems to whether they should exist at all continues to be contested (DSIT, 2024b). And all this strategic indecision has risked hampering market confidence (c.f. Joshi, 2020).

1.2.1 Two Approaches to National Identity

For policymakers, the debate has primarily concerned the relative benefits and risks of government-run systems versus private sector alternatives. As far back as 1998, the Parliamentary Office of Science and Technology (POST) (1998, pp. 60–61) recognised either "government-issued smart cards" or a series of "providers in the private sector" as the two main options. Both were intended to replace the constellation of disjointed systems that had so far sufficed. And very little has changed since.

New Labour initially opted for a scheme based on the first, *centralised* option—although some work with the private sector continued—proposing a system of national identity cards backed by a central identity register (Wills, 2008). Such a system would have allowed citizens to reliably and consistently prove who they were across different departments, improving their experience of public services while reducing fraud and administrative costs (Barnard, 2020, p. 17). But the creation of a monolithic state database would have also involved consolidating sensitive, biometric data on between 40-50 million people (Wills, 2008). In addition to concerns about cost, the massive surveillant potential of the resultant database attracted significant civil society pushback (LSE, 2005). After months of bitter debate, the scheme eventually became so politically toxic that all opposition parties pledged to undo it at the next General Election (E Whitley *et al.*, 2014, p. 207).

In 2010, the Conservative-Liberal Democrat Coalition took power and made good on manifesto commitments to put a halt to identity cards (Coalition Agreement, 2010). But this meant an alternative approach had to be found. Government would still need to wrench the state bureaucracy into the new millennium, while nevertheless avoiding the supposed authoritarian threat of a centralised identity register (Stalla-Bourdillon *et al.*, 2018, p. 787). The Coalition accordingly opted for POST's second route. Amidst a renewed wave of neoliberal enthusiasm for the private sector, *federating* the national identity system under its *GOV.UK Verify* scheme would have allowed digital identities created with corporate providers to be used across the entire economy (Chadwick, 2009, p. 3). Today, these kinds of system are common across much of the internet, where people readily sign-in to websites via third-parties like Google, Facebook, Apple, PayPal, and Amazon. But, nearly a decade and a half ago, it was a

relatively novel solution for government[3] (Crosby, 2008). The Coalition accordingly pushed people to establish identities with commercial partners, like the Post Office, Barclays, or Experian, in a marketplace for digital identity services (National Audit Office, 2014, p. 8). The deal was that government would then trust these providers to assure individual identities on its behalf (Brandão *et al.*, 2015)—a new paradigm for governmental identity provision—while also (theoretically) allowing citizens to one day reuse those same identities in commercial transactions.

Verify was, in many ways, an innovative, privacy-preserving solution. The promise of outsourcing national identification was that it would not only give people greater 'control' over their identities, but also bring government into line with private sector best-practice, driving down costs and sparking competition (E Whitley, 2018, p. 38). In reality, however, Verify turned out to be another high-profile, expensive disaster—mothballed by the Treasury a few years later (Glick, 2020b). Red and blue governments alike had foundered when it came to identity, with both of POST's options tried and failed.

Perhaps surprisingly, however, revised versions of the strategies behind both identity cards and Verify live on. In 2024, the British state is again building a centralised identity system for use across the entirety of Whitehall (Cabinet Office, 2022). And it also remains committed to establishing a marketplace for digital identities in the private sector (Prime Minister's Office, 2024b, p. 39). Both approaches will now therefore be tried together. But, despite this, almost no academic work has engaged with these two modern systems. Britain thus provides an excellent case study for exploring the numerous interrelated issues surrounding different approaches to governmental digital identity policy. Comparing the country's historical systems will allow me to analyse the different architectures of identity cards (centralised) and Verify (federated), as well as shed light on their looming replacements. But, more importantly, it will also allow me to reveal the normative risks and opportunities of each option, bringing out the interplay of politics and technology that is so critical to understanding these schemes and their travails[4].

1.2.2 Two Views of Identity Systems

There is a valuable corpus of interdisciplinary research to draw on in this task, that has already traced aspects of the digital identification landscape. The most relevant critical perspectives, for our purposes, can be divided into two camps, reflecting the central tension I have already recognised: scholars that denounce the

[3] During the identity card years, HMRC's federated Government Gateway had continued to develop in the background, pioneering much of the approach Verify would take up and develop on a grander scale (Fishenden & Mather, 2021). See Chapter 6 for more.

[4] Normativity "refers to any declaration with prescriptive or evaluative content, including statements of moral evaluation […] or prescription" (Mittelstadt *et al.*, 2015, p. 1033).

'surveillance state', and those that see the promise of the 'service state'. Identified by John A. Taylor, Merriam B. Lips, and Joe Organ (2009, p. 136), these bodies of literature respond to the "information-intensity that characterises the relationship between the modern state and its citizens" in markedly different ways. As the name implies, the first, more normatively-charged strand sees identification as a tool for greater state oversight and coercion. The literature thus connects identity policy to well-established sociological critiques of the state's administrative power—James C. Scott's (1998) concept of state legibility, John Torpey's (2000) account of states monopolising the 'means of movement', and Michael Mann's (1984) elaboration of two species of state power. Drawing on this work, others have since catalogued how states use cards, records, and computers to monitor and control populations (CJ Bennett & Lyon, 2008; Caplan & Torpey, 2001; Kerr *et al.*, 2009). And, as the name suggests, it is often the Orwellian surveillance potential of digital identity systems that is of primary political or ethical concern to these theorists. Many of the possible risks to citizens that such systems pose are therefore brought out by this literature.

The other, service-oriented strand of research is far more concerned with the potential benefits of digital identification. Work from sociologists like Manuel Castells (2009c, 2009b, 2009a) and Daniel Bell (1973) provides a more optimistic theoretical foundation, while international players like the World Bank pitch access to digital identities as a fundamental human right (Beduschi, 2019). Coming from a more administratively-minded perspective, this literature pushes for "thorough-going digital changes in administration" to allow governments to better serve their populations (Margetts & Dunleavy, 2013, p. 13). To this end, digital identification is seen as a vital tool for instituting user-focused, 'joined-up government' (JA Taylor *et al.*, 2009, p. 145). In other words, service state thinkers see digitalisation as a chance to dramatically re-imagine government, upping the quality and quantity of public services while also potentially personalising aspects of service delivery (JA Taylor *et al.*, 2009, p. 136). These scholars thus stand in stark contrast to the fears that define the surveillance state, with the downside being that they often fail to attend to digital identity's very real moral and political risks—instead seeing such technologies merely as neutral tools.

While Taylor, Lips, and Organ (2009, p. 138) tried to bring these two perspectives to bear on one another over a decade ago, I will argue for the need to transcend and update both approaches in light of modern policy. The main reason for this is that recent British digital identity systems have actually involved melding public and private actors together. Discourses predicated on the state alone are consequently too reductive—there are richer normative lenses we can draw on here, which might account for the role of corporations, while also revealing other theoretical issues at play.

1.3 Project Overview and Research Question

Despite the utility of all these bodies of literature, and others we will discuss, this thesis is primarily a response to the scant scholarship considering modern digital identity systems from a philosophical perspective. Given the importance of digital identity systems for understanding today's citizens, their evolving relationships to the state, and their dealings with businesses, one might well expect liberal theorists to have weighed-in. After all, concepts like citizenship, freedom, rights, power and equality are meant to be our bread and butter—and, as we will see, digital identity technologies are bound up in all these issues. Yet much of research instead takes what Evgeny Morozov (2013) terms a 'techno-solutionist' outlook, recommending superficial technological fixes rather than probing the interrelated normative motivations behind the drive to digitise identity systems. Indeed, with the exception of David Barnard-Wills's (2012) post-Marxist critique of New Labour's identity card scheme, no attempts have been made to explore British digital identity systems from a political-theoretical standpoint. As we will see, philosophers have only ever approached the topic of digital identity provision indirectly, or in passing. In the words of one democratic theorist, philosophers are still "playing catch-up with the fast-moving world of digital technologies" (Bernholz *et al.*, 2021, p. 5)—even though such systems hold evident relevance for any modern theory of politics.

This oversight presents us with an exciting opportunity, for political philosophy has much to offer the identity debate. At the very least, agreement on the bounds of the acceptable, and a firm sense of where the red lines are, would make finding a reasonable way forwards easier. And un-muddying the foundational, normative problems that have lurked beneath prior attempts to solve the digital identity dilemma would be an important first step. In what follows, I therefore construct a broadly-liberal framework for cataloguing, analysing, and making coherent the range of salient issues that have charged the debate over what form our identity system(s) should take. This involves illuminating the changing nature of the British welfare state, and the dominant understandings of freedom that have driven government action.

Additionally, both digitising state identification and the creation of marketplaces for identity have the potential to alter the very "meaning of citizenship" in Britain (Lips, 2013, p. 61). I will consequently consider the theoretical impacts these developments could have for the citizen's relationship to the increasingly digitalised state, as well as private companies. This will involve exploring irreducibly-philosophical questions: what freedoms and rights should people possess—whether included *or* excluded by these systems? What are the corresponding duties they might be owed? Are the institutions involved acting fairly and proportionally? And is the part-privatisation and mediation of our relationships with government even desirable in the first place?

Overall, I will argue that successive governments' lack of engagement with these fundamental questions, and the corresponding lack of justification for the decisions

they have made, has laid shaky foundations for British identity policy. This has left the civil service bowing under the weight of decades of inherited normative contradictions—with the central tension of digital identity systems still unresolved. Yet, from a properly-reconstructed, liberal vantage point, it will also be possible to recommend a more reasonable course of action, justifying my recommendations over the competing alternatives. In doing so, I will provide an answer to the following overarching research question:

What would a coherent, liberal democratic rationalisation of contemporary British digital identity systems look like?

1.3.1 Reflective Equilibrium

This brings me to my chosen methodology. Tackling a project like this, and answering this kind of question, usually involves employing the most widely-used method in philosophy—reflective equilibrium (RE) (Lewis, 1983, p. x). This approach is appealing because, unlike with some political-philosophical methods, constructing a reflective equilibrium requires the thinker to take seriously the value pluralism that is so central to liberalism (List & Valentini, 2016, p. 527). This renders it especially suitable for weighing conflicting normative concerns in the context of a mature liberal democracy like Britain. Nevertheless, finding such an equilibrium requires a lengthy process of mutual adjustment (Rawls, 2005, p. 20). The thinker begins in a state of relative naiveté and disorder, and hopes to end-up in a well-ordered and coherent end-state by going back and forth between theory and practice. To construct my reflective equilibrium, I therefore had to weave together a cohesive set of liberal moral and political principles with my considered judgements about the British identity context, to form a theoretical scaffold that retained a close relationships to the real-world, before this could eventually go on to inform political decision making[5] (List & Valentini, 2016, p. 526). It is accordingly worth saying I could only share part of this process over the following chapters—far more happened beyond what made it onto the page.

I must also flag that, traditionally, this process is carried out by the philosopher alone. However, I followed the example of a number of theorists who now recognise empirical data to be a "constitutive aspect of their arguments and theorizing" (Perez, 2020, p. 339). To me, establishing an empirically-informed understanding of British digital identity was clearly desirable. This involved gathering and examining data about the country's identity context to a) source factual information about how

[5] Although one exercise could be to design systems from scratch, that was not my goal here. I sought to take what Starmer's government has inherited as my starting point, and consider what a refined option could look like. However, to understand the present, you first need to understand the past. I therefore began by evaluating the systems we have already tried in Britain, in order to understand how we got here.

contemporary systems operate, b) help me understand the history of prior systems and why they failed, and c) allow me to collate and analyse the value-based reasons for the government's push for digital identification. In addition to desk research, I therefore engaged in reflexive engagement with a wide range of stakeholders—from civil servants and government contractors to civil society actors, academics, journalists, and critics. Through semi-structured interviews, I gathered a range of judgements and principles to inform my theory and help ensure my theoretical work was solidly grounded in the institutional reality of Britain (Baderin, 2017, p. 14). This increased the credibility and justificatory power of the resulting recommendations (De Vries & Van Leeuwen, 2009, p. 494), thereby ensuring that my analysis could lead to concrete, relevant policy proposals (de-Shalit, 2009, p. 42).

1.3.2 An Initial Position

Reaching an RE involves a journey of some kind—at least some evolution in thinking should result from all that mutual adjustment. A little unusually, I will therefore furnish readers with a brief overview of my 'initial position'. Making these starting points explicit from the outset will help orient us as the argument unfolds, allow readers to benchmark their own views against mine, and hopefully demonstrate the value of reflective equilibrium. Just over six years ago, the idea for this project was born after a summer job at Mvine Ltd., one of the companies working on the government's Verify scheme. This constituted my first exposure to Britain's difficult policy context. For reasons I will shortly elaborate upon, I could not quite believe that such a scheme was needed. Nevertheless, the role helped me see the value of getting Verify up and running, and I thought the idea of the private sector providing identity services would make an interesting case study for doctoral research. But, a year or so later, as I embarked on this project, Verify was already struggling. The project's scope therefore quickly expanded to include other possible architectures. Shortly thereafter, a historical element then also emerged as I began to realise the cultural depth of the issues at play.

Nonetheless, my early thoughts could probably be defined by a left-leaning faith in the capabilities of the British state, and indeed liberal democracies more generally. The Coalition's desire to involve the private sector in Verify was therefore genuinely puzzling. Having spent some of my formative years in countries with high levels of trust in government, national identity cards, and centralised identity registers, this is perhaps predictable. Both Sweden and Belgium—where I lived for a handful of years during my childhood—supply foreign residents and citizens alike with unique personal identification numbers tied to physical cards (Fishenden, 2005; Husz, 2018). Inclusion in each country's respective register had thus granted me and my family with access to various benefits and protections—and, indeed, was required to meaningfully participate in society. Although I was young when we lived in these countries, later conversations with my parents had nevertheless impressed upon me how easy administrative interactions were made by our identity cards. The few times

I or my family needed to rely on or interact with the state, the systems worked well, and inclusion in the national registers made it easy to access state services. In fact, the systems were basically invisible to us—cards were not really salient features of life, as they faded into the background of everyday interactions.[6]

Much the same was true in Hong Kong, where, years later, I studied abroad. Foreigners and citizens here were also furnished with biometric identity cards. But while the cards were a novelty for the Brits and Americans, few other international students seemed bothered. Although trust in government was lower—and we knew the Chinese state was likely surveilling at least some of us—the historical context of a strong colonial bureaucracy meant that such measures were not especially unexpected and noteworthy. I still only really saw the upsides of a good identity system. This now surprises me. I was, it must be said, planning to write my undergraduate thesis on the moral harms of mass surveillance. Yet it is only with hindsight that I now realise these views conflicted. This is the value of reflective equilibrium; resolutions to such conflicts are forced. But, at the time, upon returning to Britain I found my home nation's lack of similar systems hard to understand. Digital registers seemed like the bare minimum required for a functioning, modern government. Britain felt decades behind Scandinavia, in particular. Since 1997, after all, Sweden's 'personnummer' register and BankID system had empowered citizens to live flourishing lives, like similar schemes across all of the Nordics (Husz, 2018). Still today, there is no British equivalent. As discussed, a melange of fragmented, interlocking systems across instead provides a rather less cohesive functionality.

Over time, as I interacted with more of the state and other important institutions, I was consequently faced with what I perceived as the preposterousness of needing to carry documents such as my birth certificate to 'prove' who I was. These feelings reached their peak during the coronavirus public health crisis. I vividly remember fulfilling my 'right to rent' obligations—a requirement for tenants to confirm their legal right to residency in Britain—by video-calling an estate agent and holding up my driver's licence. The idea that this charade constituted a rigorous identity check, and that a card that allowed me to drive was appropriate for the task, seemed absurd; I could have held up a completely fabricated document and they would have been none the wiser. Why could the government not just give us all a proper identity card and have done with it? Having been too young to witness much of the identity card debate of the early 2000s, I was unaware at the point that there had been such civil pushback—and it was only as I got deeper into my research, in the years to follow,

[6] I migrated as a white, cisgendered English speaker in a relatively comfortable socio-economic position. I recognise that migrants coming from different contexts, especially those experiencing intersecting forms of oppression (c.f. Crenshaw, 1989), may well have struggled to find similar levels of recognition and acceptance in the eyes of the state.

that I finally understood the long history of identity resistance in Britain. As you will see, my views now are consequently more nuanced.

1.4 Key Contributions and Significance

In sum, this thesis fills two intellectual niches—expanding our understanding of current schemes while simultaneously reinterpreting much of what has come before, through the lens of political philosophy, for the first time. In addressing the latter oversight, I construct a novel, liberal-democratic understanding of British identification policy by reinterpreting work on prior systems. I therefore hope that theorists interested in the state and the nature of its relationship to citizens, as mediated by administrative systems, will find much to discuss. This work involves bringing together various normatively-relevant aspects of existing literatures, drawn from neighbouring disciplines, at the level of political-philosophical analysis. Research from other fields provides a pregnant, interdisciplinary basis from which to build out my critique. And, although such an understanding of the normative specifics of our national digital identity systems may only seem to be of concern to philosophers, it should in fact be of concern to anyone living in Britain. After all, if digital identities continue to gain in popularity, they could become the default or even only way in which we interact with the state. Unearthing shared theoretical ground upon which a mutually-acceptable solution might be built is thus vital work. What are the foundational normative issues underpinning the current digital identity debate in Britain? Where do they stem from? How can they be resolved?

Extrapolating from the past—with a mind to both what is technically, as well as culturally, possible—I then ultimately recommend a path forwards. This tackles the former niche: the paucity of research evaluating modern national identity schemes in Britain. Although legal scholars, social scientists, computer scientists, and information systems researchers have all published widely about prior solutions, by contrast the contemporary policy direction has attracted little attention. This is despite the fact that, after twenty-five years of development, the British state still lacks a system fit for supporting a modern digital bureaucracy (Morton, 2024). Indeed, when I began writing this thesis, the country's digital identity policy seemed caught in a death spiral—and, since then, another system has ended in failure. Many consequently appear to have lost interest. This has left the modern replacements for these failed systems to develop without attracting much, if any, critical evaluation. In appraising these replacements, I therefore detail many aspects of current policy, and the likely effects for citizens, for the first time. But, more importantly, I also recommend making a series of changes to these systems, driven by well-founded theoretical commitments. This primarily stems from a reconceptualisation of digital identities themselves. In addition to philosophers and academics who have previously published on identity, then, a further key audience for later chapters is the policymakers and politicians who may have the ability to chart a more coherent course if these foundations can be stabilised, lessons learned, and appropriate changes made.

Finally, to this end, political timing has also conspired to make this thesis significant. Following fourteen years of neoliberal austerity under Conservative governments, the Labour Party took power in July 2024 after a snap election (Prime Minister's Office, 2024a). As I write, it is too early to tell what kind of government Labour's will turn out to be—but, regardless, changes of administration are always a moment to step back and reflect. While this thesis cannot of course, on its own, solve the identity issues Britain faces, outlining a rational basis from which a coherent liberal policy could progress, defended in such a way that many stakeholders will find the conclusions acceptable, should at least make figuring out the next steps easier. No doubt my proposals will not please everyone, but pluralistic societies are built on compromises that can be mutually tolerated for principled reasons.

Whatever comes next for British digital identity policy, I will nevertheless have brought together and clarified several important strands of the debate—at a level that the public conversation has so far overlooked. This is novel work. While parts of the greater whole I construct have been previously analysed, no one has yet brought them together in a political-theoretical project such as this. Overall, I hope readers will consequently agree that political philosophy has much to say about digital identity systems, and that there is much to be gained by bringing normative theory to bear on the technologies that have become so important for citizenship in our modern society.

1.5 Thesis Outline

Including this introduction, this thesis comprises nine chapters split across three parts, plus references. *PART I* begins by situating my argument and outlining my methods. *Chapter 2*, the literature review, defines our key terms, then summarises relevant work on the liberal state and (digital) identification technologies, locating my project at the intersection of these (so far) almost entirely separate strands of research. A focus primarily emerges on questions relating to citizens, their freedoms and equality, their relationships to the state and other key institutions via various identification apparatuses, as well as the normative impacts of these technologies. Overall, I emphasise how the lack of a political-theoretical approach has stymied prior attempts to systematically structure and unpack the problem space. *Chapter 3* then details the version of reflective equilibrium I used to build a liberal political philosophy of British digital identity systems and address this shortcoming. I combined a relatively traditional implementation of the method with material gained via a series of elite interviews. Testing and refining my ideas with these stakeholders helped me to gain a greater empirical sensitivity to the normative issues, while bringing to light my biases and blind spots. This ensured my theorising remained tightly tied to reality—with the hope of ensuring relevance for the current context.

PART II then comprises the core of the original research, forming something like a 'normative history' of British digital identity systems. I first assess prior, analogue identification systems in Britain, to contextualise later discussions, before turning my attention to the state's first two attempts to build a national digital identity system. In

each chapter, I extract key insights for a liberal political philosophy from successive governments' attempts to implement different systems. Canvassing the long stretch of the Industrial Age, *Chapter 4* surfaces the dramatic changes for the citizen-state relationship in Britain that accompanied governments making the population legible through non-digital systems. It details what I see as the inherently discriminatory nature of identity systems, alongside the progressively greater state interference that accompanied new identification technologies, first abroad, then at the borders, and finally in the streets. *Chapter 5* then explores Britain's first nation-scale digital system, asking what changes when these systems are digitised. Politicians and policymakers generally promise faster, more efficient and secure access to services, with a reduction in fraud. But I also show how central identity registers can further state surveillance and the coercive control of populations. *Chapter 6* then discusses the state's second attempt to realise these benefits via a more privacy-preserving architecture. Nonetheless, I criticise the marketisation of state identification this entailed as well as rampant inequality it countenanced, drawing on critiques of neoliberalism.

In *PART III*, we at last turn to Britain's contemporary digital identity systems. In *Chapter 7*, I show how the government's current identity policy blends elements of what has gone before into a new whole. Taking this as my starting point, I then construct a coherent equilibrium that can respond to the points raised in prior chapters. Although this cleaves fairly closely to the inherited status quo, I do propose several key ways in which the government could revise policy and build systems to address the interlinked issues identified in previous chapters. This includes preventing the conflation of digital and algorithmic identities, solving the inclusion problems that have dogged modern British systems, and preventing the economisation of identities in the private sector. I also advance a novel philosophical understanding of digital identity provision as a kind of instrumental good. In *Chapter 8*, my last, I then provide an overview of my conclusions and policy suggestions. As often happens, the relationship turns out to be dialectical: not only does liberal political philosophy have much to say about digital identity systems, but appraising these systems also has import for longstanding issues in political philosophy—the technological systems that mediate our relationships with the state have, thus far, been overlooked. In closing, I then identify future avenues for further research and evaluate my overall project, suggesting areas for further improvement.

—Part I—

Chapter 2.

Literature Review

> "Everywhere the State acquires more and more direct control over the humblest members of the community and a more exclusive power of governing each of them in his smallest concerns. This gradual weakening of the individual in relation to society at large may be traced to a thousand things."
>
> *– Alexis de Tocqueville (2004)*

Digital identity systems are becoming fundamental tools of modern governance[7], altering centuries-old identification practices (Sullivan, 2011, p. 9). As we will see, they raise difficult, inherently-political questions to do with asymmetries of information and power, access and control, citizenship, democracy and rights, as well as privacy and security. But, over the course of this chapter, I will show how—despite the wealth of normatively-salient issues surrounding digital identification, particularly when deployed by states—almost no research has so far engaged with the technology on a political-philosophical level. While academics in other disciplines have wrestled with some of these questions in isolation, political philosophers have remained on the sidelines. And many gaps in the literature remain. Indeed, it was only around the turn of the millennium that identity systems, digital or otherwise, became a topic of concerted study amongst scholars at all. As a result, identity's "significance has almost gone un-noticed as our highly complex and interdependent technological society has evolved. It is only with the debate surrounding ID card systems and the rise of Internet and electronic fraud that there is any awakening" (Collings, 2008, p. 62). Important work from other disciplines provides a strong start, but there remains a real need for political philosophical guidance around the design and implementation of digital identity systems.

[7] Identification really is becoming fundamental for digital states, as the largest biometric digital identity system in the world, India's 'Aadhaar', well illustrates. The scheme's name, which translates to 'foundation' in most Indian languages, succinctly communicates how society is expected to build on a basis of identity services (Ramnath & Assisi, 2018, pp. xxix–xxx).

This chapter accordingly grounds the argument to come, defining key terms and summarising what we can learn from existing research into digital identity systems—in Britain and abroad. I first canvas relevant work from multiple literatures to draw out the range and scope of normative issues that need tackling. Then, I make clear what a liberal critique can add to our understanding of national identity policy, particularly by addressing the limits of the current debate. A central aim of this thesis—to evaluate British digital identity systems through the broad lens of liberal theory—thus emerges. In this task, I am helped by the fact that (political) philosophers and philosophers of technology have already advanced critiques in similar but distinct contexts that can be readily extended to digital identity systems. This chapter consequently concludes with an overview of my basic liberal-theoretical framework, highlighting the central values at play in the identity debate from a liberal perspective: liberty, equality, and the role of the market. I also discuss the liberal conception of citizenship which underpins these values. With this in hand, over the remainder of the thesis I will propose a number of ways to resolve the interlinked normative contradictions that have dogged these schemes and their implementation in Britain.

1.1 Terms of the Debate

This thesis is about digital identity systems, specifically those developed by successive British governments. However, such systems are multifarious and complex—there is no one archetypal digital identity system. From the outset, I must therefore clarify that, when I talk about digital identity systems, I am referring to *those that enable digital means of personal identification to public or private institutions as part of a national identity scheme*. In other words, I am only concerned with a subset of the whole range of computerised systems that manage individuals in Britain based on who they are and what they are eligible to do. Immediately, this places some topics beyond the terms of engagement. I am not, for instance, concerned with the identities of non-human entities—such as organisations, Internet of Things devices, or even agential artificial intelligences—much as some identity systems happily accommodate them (Kent *et al.*, 2003; Wachter, 2017). Neither am I particularly concerned with the 'Identity and Access Management' systems companies use to manage employees or customers, except where these technologies have influenced national identity programmes. What we will, instead, primarily focus on are those systems that states—and, occasionally, companies working on behalf of the state—use to register, identify, authenticate, and authorise people, in order to control their access to goods, rights, liberties, citizenship, services, and recognition. Before we can get into further specifics, though, we need to first agree some other basic terms.

1.1.1 Specifying Digital Identity

Digital identities themselves are a good place to start. Sociologists, psychologists, computer scientists, and philosophers have all had much to say about identity in the broadest sense (Bertino & Takahashi, 2011, p. 22). It is a concept that has been debated since antiquity—but also, to borrow a phrase from Daniel J. Solove (2008), a concept

that is now in disarray. Today, the term is used liberally across different disciplines and literatures, covering anything from personal identity construction in social contexts, cultural identification within groups, to the more technical solutions that primarily concern us here. Thus, when I refer to 'my identity', I could mean everything from an identifier, like my name, Charlie Smith, to how I perform my personal identity, online or offline, or how I identify as a doctoral student or British citizen. But I could also be referring to how I might prove any of these claims, be it with my student card, passport, or even digital credentials like my institutional single sign-on or a digital diploma. These are all facets and artefacts of my identity. And while significant scholarship surrounds these different versions of the concept, the boundaries between them are not always clear. Additionally, our case is not helped by the fact that many socially-salient aspects of an identity are not captured by the tools and mechanisms of the state's identification systems. Yet we can make some useful distinctions here to get the ball rolling.

As a philosopher, it is of course hard to resist a reference to the *cogito*—but resist I shall. Instead, it is to another French *philosophe*, Paul Ricoeur, we will first turn. Ricoeur (1994) was concerned with the relationship between the concepts of identity and the self, and the ways in which we use the term 'identity' to pick out these interrelated yet distinct concepts. He distinguished between two kinds of philosophical identity. On the first understanding, our *idem* identity is that which never changes. This form captures the categorical and hierarchical "significations" that define us over time (Ricoeur, 1994, p. 2). Modern democracies consequently provide a series of rights and protections in relation to many of these categories, like race and sex. Among other purposes, this means idem identity maps to the categories that get recorded on things like our identity documents because they consistently pick us out throughout our lives. By contrast, the other form, *ipse* identity, is defined by change. This sense of identity captures the narratives or stories that we tell ourselves about who we are now and how we have evolved, even if we remain the same self underneath all those constant changes (Ricoeur, 1994, p. 3). The person I am today is the same 'me' that started this project, even if many of my views have altered and I no longer see myself in the same light. In democracies, rights to self-expression and privacy protect this sense of self, allowing us to tell stories about who we are over the course of a lifetime.

Although Ricoeur was talking about philosophical notions of identity, the digital identity literature also bifurcates along his two main lines of distinction. The first, idem sense is most relevant for us, according to which a digital identity is a tangible yet artificial 'thing' that people possess. An identity is, in other words, "a set of claims made by one digital subject about itself" (Cameron, 2005, p. 4). On this view, an individual's identity amounts to the bundle of data within a digital system that uniquely describes them, as well as their relationships to other relevant entities (Windley, 2005, p. 8). More technically, digital identities are constituted by data that allow individuals to be distinguished from one another; an identity is precisely "the

dynamic collection of all attributes related to a specific entity" that enables their disaggregation (Collings, 2008, p. 62). The benefit of such identities is that they can be 'held' and presented by individuals seeking to make claims about who they are, without relying on equivalent physical documents or artefacts such as utility bills and passports. Authorities, whether private or public, can check these identities to ensure that only the right individuals gain access to a system, entitlement, or piece of information (Lyon, 2009, p. 9).

A digital identity can thus essentially be thought of as a digital version of an identity card. We might, alternatively, think of a digital dossier of identity-related facts about a person. But a digital identity is far more than a digitised piece of paper, card, or plastic (Bertino & Takahashi, 2011, p. 12). It might include names, numbers, permissions, logins, or even face scans and fingerprints. Whenever I talk about 'a digital identity', I will therefore be referring to the bundles of credentials, attributes, identifiers, and biometrics that can together distinguish unique individuals—though it is worth remembering that each identity system is likely to store a different combination of these elements.

As one might expect, the existence of digital identities relies on a series of processes to create and manage them. First, the process of *identification* involves picking out a unique individual and storing information about who they are, tied to a unique identifier (Otjacques *et al.*, 2007, p. 33). This is closely related to, and fundamentally involves, an individual's digital identity, even if the two concepts are not equivalent. By contrast, the subsequent processes of *authentication* and *verification* do not explicitly identify people, but instead ask whether someone asserting a claim to a digital identity here and now is the same person that claimed the identity in the first place (Lyon, 2009, p. 115). Finally, *authorisation* again asks not who you are, but rather what you can do in light of an identity's associated permissions (Kent *et al.*, 2003, p. 20).

As my above focus on idem identity no doubt betrays, the other kind of 'digital identity'—an individual's digitally-mediated ipse identity—is almost entirely unrelated to our purposes. This concept instead captures how people intersubjectively present aspects of their personal identities online (Feher, 2019, p. 2). To update Erving Goffman's (1959) work for the digital age, we might say that every time someone socially performs their identity on the internet, they leave digital traces of the persona they are trying to cultivate (Hogan, 2010). Just think of somebody's posts on Facebook, Instagram, TikTok, or X (formerly, Twitter). In aggregate, these performances amount to a digital manifestation of their personal identity (Bullingham & Vasconcelos, 2013)—one that will naturally change over time. But while this second understanding of 'digital identity' may occasionally overlap with the first, as the digital traces we leave online can be used to surveil and track us (Raab, 2009), it is nevertheless not my concern in this thesis. These identities are extrapolated for profiling and marketing purposes, not minted by institutions for people to carry and present in formal identity

interactions[8] (CH Smith, 2020). And it is this latter means of individual identification by digital systems that I am principally investigating—even if the profiling carried out under contemporary informational capitalism can also form a source of data for identification purposes (c.f. Couldry & Mejias, 2019). Idem identity, not ipse considerations of the self, will accordingly be the salient concept as we evaluate the British state's various identity systems[9].

1.1.2 Why National Systems?

In the abstract, I dare say that digital identities are not particularly interesting. Anyone could, in theory, make me a digital identity, in their own system and for their own purposes. But, while this may raise some privacy or consent issues, there are not necessarily deep political or moral dimensions to such an action. However, as we have already seen, when states and other important institutions deploy such systems, the normative stakes are raised. It is these systems that consequently attract my attention; the digital identity-related mechanisms that powerful, political actors create and use to administer society.

This quickly gets us into more normative territory. For one, questions of what makes a good or bad system come straight to the fore, given the impacts such systems can and do have on individuals' lives. In other words, it redirects our attention from the digital identities themselves to what Gilad Rosner (2014, p. 98) calls the *identity management policies* that define such systems: "the set of laws and policies enacted by governments and supranational bodies concerning the facilitation, procurement, use, liability, legal nature, interoperability, technologies, risk methodologies, lifecycle and privacy of digital identities for its citizens". It is the decisions states make and encode in these policies that conditions the effects digital identity systems have on people—much like with any other powerful technology. An embryonic connection to more political-philosophical questions thus begins to emerge.

1.2 What We Know About Digital Identity Systems

So, what are the contours of the contemporary digital identity debate? From the off, it must be said that the intertwined moral and political complexities of identity policy simply do not feature as a concern in many fields. While this is understandable, it does mean these literatures are less relevant for this project. The main example in this category must be the technical and standards-setting literature. While there is an extensive body of work cataloguing technical considerations of identity systems—examples include the specifics of credential design (Alpár & Jacobs, 2013), engineering

[8] They are not "organisationally governed" for the purposes of identity management (Rosner, 2014, p. 92).

[9] The distinction has also been framed as the difference between 'identity' and 'identification' (Krajewska, 2017, p. 18).

challenges surrounding unique identifiers (Andrew Martin & Martinovic, 2016), and the resilience of ePassport protocols (Avoine *et al.*, 2016)—computer scientists, through no fault of their own, largely neglect to consider the associated political and ethical issues at play. This renders their work less relevant for my purposes. Whatever technology is used, it is the *impacts* of these systems upon people that defines them in normative terms. Thus, in the chapters to come we might discuss the benefits of a privacy-preserving system, the inclusion issues associated with a policy, or the possible illegality of non-consensual registration—but not the relative effectiveness of encryption algorithms or the levels of interoperability a particular standard can achieve. It is the former aspects that have, so far, been understudied, and there remains space to make a significant contribution by discussing identity technology at the functional rather than technical level.

Technical scholarship aside, we can pick out several further literatures that will be of limited import. The first of these is empirical case studies situating digital identity systems in their respective social and political environments. The classic example here is Estonia's X-Road programme which, although impressive, is widely acknowledged to have developed in a quite disparate context to that of Britain, making it hard to draw lessons (Margetts & Naumann, 2017). But the problem goes beyond the Estonian example. While much work looking at other countries does have a normative slant, it too does not easily translate to the British case. For instance, we can look to the persecution of the Rohingya people in Myanmar via identification systems (ISI, 2020), surveillance and exclusion in India's Aadhaar system (Khera, 2019; Ramnath & Assisi, 2018) as well as China's social credit system (Orgad & Reijers, 2021; Trauth-Goik & Bernot, 2021), or digital identity-related voter suppression in Chad (Debos, 2021), but it is not obvious how much more than general insights can be extracted from these empirical examples. Some of these countries are not democracies, or liberal, and others are pursuing identity models that have already been tried and failed in Britain, or else are not feasible here for other reasons. Their contexts are therefore far removed from that which I am are considering—meaning only vague warnings around, say, the exclusionary and surveillant potential of certain kinds of digital identity systems can be extrapolated. And, while those lessons can and have been learned, the wider applicability is limited.

Next, certain kinds of legal and regulatory contributions will also be out of scope. Some lawyers have long recognised the importance of digital identity systems (c.f. Sullivan, 2011). As Lawrence Lessig (2006, p. 45) argued almost two decades ago, "We're far enough into this history to see that the trend toward this authentication is unstoppable. The only question is whether we will build into this system of authentication the kinds of protections for privacy and autonomy that are needed." Occasionally, legal scholarship does therefore consider the political values at play in identity systems—and so will inform my work. But other tranches, particularly those analysing legal regimes and directives (e.g., Roberts, 2015), will not be considered. I am, after all, concerned with what *ought* to be done about digital identity systems. This

is a very different question to what is legal at a point in time. The law in Britain may well need to change to accommodate a normatively-acceptable policy position, but we can only know this once we have a preceding understanding of what values the law should espouse[10] (Mittelstadt *et al.*, 2015).

Finally, it is also worth mentioning the wide array of work that details corporate applications of digital identity systems in various different situations. This includes contexts as diverse as financial services (Mario Lavizzari *et al.*, 2021), healthcare (Falcão-Reis & Correia, 2010), gambling (Carran, 2018), and more. Again, while the questions of access that run through all identity systems may have some moral or political implications here, on its own this work tells us little about digital identity in relation to British national identity policy and the associated concerns relevant to statehood, citizenship, and various liberal values. These contexts are ruled by questions of technical optimisation and better service design. They do not concern the fundamentally-political considerations that motivate this project. As a result, they, too, will largely be set aside.

1.2.1 Normative Analyses

Despite having bracketed off these literatures, there are still many other avenues for us to draw on. Most pertinently, questions around the acceptability of digital systems for governing populations are central to academics situated at the burgeoning intersection of critical development studies, science and technology studies (STS), and sociology. The cluster of normatively-charged research that has grown up around the deployment of so-called 'foundational' digital identity systems in development and migration contexts is highly relevant (Cheesman, 2022b; Gillespie *et al.*, 2018). Much of this scholarship responds to the United Nation's pursuit of Sustainable Development Goal 16.9, which seeks to achieve 'legal identity' for all by 2030 (Beduschi, 2019). Many countries have interpreted this goal in explicitly digital terms—an interpretation that is not uncontroversial (Manby, 2021). The result has been an emerging orthodoxy around digital identity's importance for development (c.f. Gelb & Diofasi Metz, 2018), with many countries pursuing radical plans to digitally integrate and legally register citizens via computerised identification systems at breakneck pace. India's Aadhaar system, for instance, has already assigned well-over one billion unique identifiers, linked to individuals' biometrics, to people all across the country—despite drawing considerable dissent from researchers (Hosein & Whitley, 2018; Khera, 2019). Discussions around what constitutes responsible digital

[10] Indeed, Charles Raab and Colin J. Bennett (1998, p. 256) have argued that existing data protection law and regulatory policy can often be inadequate for the philosophical evaluation of emerging information technologies, because knowledge of due process as it stands is not enough to secure good and right substantive outcomes.

identity usage in these contexts have accordingly come to the fore[11] (Anand & Brass, 2021; Masiero & Arvidsson, 2021).

The most normatively-charged research often approaches these systems through the lens of *data justice*. Governance scholar Linnet Taylor (2017) has defined this in terms of "fairness in the way people are made visible, represented and treated as a result of their production of digital data". Work in this vein therefore often draws attention to the ways in which digital systems can worsen existing vulnerabilities, for example the exclusion that results from being omitted from digital civil registration drives (Gangadharan, 2021; Aaron Martin & Taylor, 2020). State identity systems are, after all, mainly concerned with discriminating between those who should or should not be recognised as citizens—meaning those left behind can be significantly disadvantaged (Beduschi, 2019). As this suggests, digital identity systems also generate issues of consent, and can exacerbate power asymmetries between individual people and the state. This is especially the case when submitting to digital systems is a precondition to securing state support. For instance, some of the world's most vulnerable populations have had their access to rations made contingent upon submitting to an experimental blockchain-based UN identity system (Cheesman, 2022a). And, in India again, the Aadhaar-based social protection system has led to claims of 'informational injustice' amongst farming communities (Masiero & Buddha, 2021). While applied in different contexts, much of this work is consequently relevant—as we will see, similar questions of equality and justice emerge in the British case, too.

The development literature also links identity systems to the development of individual liberty, usually in line with the capabilities approach (Masiero & Bailur, 2021; Schoemaker *et al.*, 2020). Foundational digital identification systems are often pitched as the necessary "platform" upon which whole new digital government ecosystems must be built to support wider development goals, opening up new ways for citizens to thereby develop material security and individual autonomy (Eaves *et al.*, 2019; O'Reilly, 2011). The capabilities approach, which found its start in philosophy but was developed in collaboration with development scholars and practitioners, accordingly connects these systems to a particularly-positive understanding of liberty (more on this below). But the impacts of identity systems for other understandings of liberty are worth evaluating, too. Another key normative angle to follow-up on will therefore be exploring the import of identity for freedom in more detail, especially in the unique case of Britain. While development scholars can, after all, draw our attention to how capabilities are limited or enhanced by foreign systems, we need to evaluate how systems in Britain, which often follow a different

[11] The Alan Turing Institute's trustworthy digital identity programme, which launched in 2020 partly in response to the international pressure of SDG 16.9, seeks to promote positive identity systems design along similar lines (Turley, 2020).

technical model to those deployed by UN- or World Bank-affiliated projects, could have differential effects.

Work in the wider STS space is likewise of interest, albeit often indirectly. This sociologically-oriented literature "offers a challenge to the liberal conception of the sovereign individual" unmoored from their surroundings (Schoemaker *et al.*, 2020, p. 18). Post-humanist STS theorists such as Bruno Latour (1993) and Donna Haraway (1988) have drawn valuable attention to how differences between individuals are partially constructed by their relationships with states and technical systems—rejecting that these categories are in any way objective or universal. Knowledge production is, rather, always political and subjective, to the benefit of some over others. Digital identity systems thus have clear relevance for this work, as they are a tool for understanding and managing populations, even though the main actors in the STS space have not engaged with identification directly. The post-humanist lens would accordingly ask us to explore how identity systems make humans up in a particular way. In Langdon Winner's (1997) philosophical terms, technical systems are understood to have a definite "politics", and do not exist as pure, neutral tools. Some technologies therefore lend themselves better than others to more democratic or more authoritarian ends. This is especially true for political technologies, such as those the state bureaucracy uses to shape its populations (Cohen, 2012). Identity systems might well therefore contribute to easily-managed, docile populations—a subtle form of discipline and control that follows from submission to these systems.

Finally, this brings us to the multiple practices involved in making citizens 'knowable' to the state bureaucracy via technologies of surveillance in particular. In line with the STS literature, sociologists and geographers have long recognised how public sector epistemologies that are too data-driven can have reductive effects, simplifying the complexities of society to categories that suit bureaucracies (Amoore & Piotukh, 2016). The decisions made using these data, often far from the frontlines of politics, can then have drastic effects for people on the ground (Amoore, 2011). The best articulation of this has perhaps come from Scott's (1998, p. 183) seminal *Seeing Like a State:*

> Any substantial state intervention in society […] requires the invention of units that are visible. […] Whatever the units being manipulated, they must be organized in a manner that permits them to be identified, observed, recorded, counted, aggregated, and monitored.

It is therefore partly through new identification technologies, amongst other surveillance technologies, that the modern state has garnered the considerable administrative power that it today enjoys. In Scott's (1998) phrasing, such technologies

make people more legible, in terms the bureaucracy can process[12]. Although anything the state may wish to better manage can be made legible, my primary concern will be the extent to which individuals have been made transparent to the state. By contrast, "the premodern state was, in many crucial respects, partially blind; it knew precious little about its subjects, their wealth, their landholdings and yields, their location, their very identity" (Scott, 1998, p. 2). This blindness limited its ability to know, and thus to act. While renowned sociologists like Max Weber and Anthony Giddens had already noted the importance of writing and filing for growing the administrative power of states (see Torpey, 2000, p. 15), Scott's insight was to emphasise how making the world legible relies upon forcing an often messy, organic reality to fit the rationalised and ordered designs of bureaucratic systems (Fourcade & Gordon, 2020, p. 1). This is a translational process, which distorts and contorts the subjects being made legible to fit prescriptive taxonomies. The link with the STS literature, which has likewise gone on to adapt and develop understandings around the systems of state 'knowing', should thus be evident.

1.2.2 The Surveillance State

At this point, it is worth stressing that, today, there is no dedicated field of study for national digital identity systems. Identity is, at most, a tangential interest for development scholars, who are far more interested in the effects of these systems. Yet, as identity proposals filtered into governmental briefs and corporate systems proliferated in the early-2000s, a discrete digital identity literature did almost define itself within the STS movement. Much subsequent work has built upon this basis, even as interest in identity systems dwindled in the 2010s. It is consequently worth discussing at length. The dominant critical perspectives here divide into two camps: those that denounce the 'surveillance state' and those that sympathise with the 'service state'. As mentioned in the last chapter, these dual bodies of literature each respond to the "information-intensity that characterises the relationship between the modern state and its citizens" in markedly different ways, and were originally identified by Taylor, Lips, and Organ (2009, p. 136). And, although a dedicated field of study ultimately failed to take root, in combination with the work above the resultant literature nevertheless provides a pregnant, interdisciplinary basis from which to begin building out a political-philosophical critique of digital identities—especially, as we will see, when combined with relevant philosophical work.

As the name suggests, proponents of the surveillance state perspective mainly emphasise the potentially invasive, restrictive, or even dystopian effects of digital identity systems (JA Taylor *et al.*, 2009, p. 137). They chiefly focus on how

[12] Legibility, of course, cuts both ways. Not only do 'the people' need to be rendered in informational terms that the state machinery can efficiently process, but mass literacy—not least amongst administrators—is a necessary precursor to widespread technical identification practices (Caplan & Torpey, 2001, p. 2).

governmental abuse of such systems could undermine citizens' privacy and freedoms—and even democracy. It is therefore perhaps unsurprising that this outlook is often shared by civil society actors and other critics of 'big' government. As we will see, the literature is also more normatively-charged than that of the service state perspective (JA Taylor *et al.*, 2009, p. 136), though this normativity grew gradually. Initially, a small group of historians and sociologists traced the development, by states and other important institutions, of pre-digital identification technologies such as papers and physical identity cards. This initial work was largely descriptive in nature, yet nevertheless drew on long-established critiques of state power that well-predated digitalisation. But the critical tenor of this work became increasingly normative as attention moved to the growing push for government digitisation at the turn of this century—not least because digitisation is generally understood to have enhanced the surveillant potential of prior identification practices.

Undoubtedly one of the most influential early contributions was Torpey's (2000) *The Invention of the Passport*. Torpey focused on identification systems from a historical and sociological perspective, and so did not really touch on modern, digital systems. But his work does powerfully highlight the significance of analogue identification systems for understanding the changing nature of the citizen-state relationship throughout the Industrial Revolution. In particular, he draws attention to how many states progressively 'embraced' their citizens via identity-related papers and cards during the period. Clearly echoing earlier theorists like Weber, Torpey argues that states exerted power to "monopolise" the "legitimate 'means of movement'" via the introduction of travel documents, and thus distinguish legitimate citizens from foreigners (Torpey, 2000, p. 2). His account accordingly emphasises how identification systems are vital for understanding both citizenship and the foundations of the modern liberal state—especially, as we will later see, in much of mainland Europe. Along similar lines, Valentin Groebner (2007) has advanced a history of the documents, seals, stamps, and signatures that the bureaucracies of Early Modern Europe used to identify and surveil citizens and foreigners alike—another valuable contribution.

Just a year after Torpey's initial contribution, however, Jane Caplan would join him to co-edit Documenting Individual Identity (2001), another predominantly historical volume. Again, their focus was neither especially digital nor philosophical, and most contributions did not focus on Britain, save for a few exceptions[13]. There are multiple chapters here with a strong normative bent, however, that begin to advance a narrative of suspicion around identity systems. A few years later, a similar collection from Carl Watner and Wendy McElroy (2004) recorded various arguments for

[13] A chapter from Jon Agar (2001) noted how 'Britishness' has traditionally preached a general distrust of national ID cards; Anne M. Joseph (2001) catalogued Victorian attempts at criminal identification; and Torpey himself (2001) further detailed passporting in World War I.

outright resisting identification systems. Histories of resistance clearly raise more political questions about identity but, again, philosophers and a focus on explicitly digital technologies were both missing—and the content was still largely descriptive. A good example is Keith Breckenridge's (2014; 2012) groundbreaking work looking predominantly at historical identification systems in the South African context. Tracing colonial histories, Breckenridge reveals the often authoritarian motivations behind attempts to control populations seen as 'lesser' by the state. He also importantly connects the analogue systems of the past to modern digital systems. This is critical work, but at no point does Breckenridge attempt to resolve these issues by proposing how these systems should be designed, at the level of political philosophy.

Nonetheless, the literature was in its ascendance at this point. By the late 2000s, digital identity systems were receiving critical attention of a more earnestly normative nature—albeit still not from philosophers, but rather sociologists—as identity was drafted into the well-established 'surveillance studies' and 'surveillance society' literatures. An edited volume from Colin Bennett and David Lyon (2008) was the first to take this step, and paid close attention to the monitoring potential of identity cards, national registers, and biometrics. Concurrently, Canadian legal scholars connected identity to the 'networked society' discourse, especially concepts like anonymity and privacy, in interdisciplinary texts like Lessons from the Identity Trail (Kerr *et al.*, 2009). These researchers all brought with them a general scepticism around ongoing state attempts to gather, process, and make use of identity data in large central databases. And, rather than just describing these efforts, they explicitly problematised digital identity systems by linking them to the state mass surveillance programmes that had proliferated in the wake of the 9/11 terror attacks in America. This is accordingly where the surveillance *state* perspective emerged for Taylor, Lips, and Organ.

For our purposes, the hardening of critical opinion around digital identification technologies during this short period is certainly noteworthy. Although prior analogue identification techniques were by no means seen as unproblematic—historians had effectively recorded their myriad issues—digital systems and the new possibilities represented by 'unblinking eyes' and automated, computer-based control of populations brought a newfound urgency and normative potency to the literature. There was a real sense that effective academic analysis might be able to influence the development of more acceptable technologies. While the papers and passports of yore may have been tools of control, their power was a) a topic of historical study, and b) mostly confined to discrete sites of interaction with officials. Digital identities, by contrast, could usher in more pervasive and diffuse mechanisms for tracking and managing populations; and potentially introduce identification requirements to areas that had heretofore been unencumbered by state oversight[14]. Negatively-charged

[14] It is probably no accident that this development coincided with growing popular awareness of the 'NO2ID' movement that opposed the development of Britain's computerised identity card scheme

images of an ever-watchful Orwellian Big Brother state consequently appear in much of this writing (Breckenridge, 2008; Ogura, 2006), drawing on the notions of 'panopticism' developed by philosophers Jeremy Bentham (2010) and Michel Foucault (1991). And these insights have since been taken up by sociologists like David Lyon (2006) and Zygmunt Bauman (2013). This was far closer to academia as activism than the descriptive histories that had preceded this work.

Yet, despite general recognition that "[i]dentification is the starting point of surveillance" (Lyon, 2009, p. 4), the works I have listed largely exhaust the surveillance state perspective on digital identity systems. Indeed, critical interest seemingly dried up around the 2010s, and identification is now largely taken for granted in much of the contemporary surveillance studies literature—with two main exceptions. The first is a recent body of work that concerns concepts like 'algorithmic identity' (Cheney-Lippold, 2011, 2017), 'digital dossiers' (Daniel J Solove, 2004), and 'data doubles' (Haggerty & Ericson, 2000)—concepts that relate more to the second, ipse strand of digital identity I defined at the outset; profiling rather than identification. This kind of surveillance does not necessarily rely on "a pre-established user identity" (Milano *et al.*, 2020, p. 962), instead recording and sorting features of our digital interactions into profiles abstracted for purposes like advertising (Søe & Mai, 2022, p. 492). Users are no doubt surveilled, processed, and categorised. But they are not usually identified nor given digital credentials to present. This literature is consequently only tangentially relevant to our enquiries. In sum, however, the surveillance state view will have much import for the critique to come in this project—particularly with recognition for how much of this work has since been drawn on by development scholars since.

1.2.3 The Service State

So, what can we learn from the opposing view? Service state thinkers mostly see digital identity systems as genuinely positive policy developments. The state's relationship to its citizens, as the name implies, is taken to be one of service and enablement, rather than watching and control. To support those aims, digital identity technologies are accordingly read as intended to allow people to more easily and securely authenticate themselves in the eyes of the state, particularly when accessing services remotely (Alan W Brown *et al.*, 2014). One of the key reasons for this is that digital identification is taken to be a vital stepping stone for any administration looking to realise the evergreen Whitehall policy goal of 'joined up government' (JA Taylor *et al.*, 2009, p. 145). Notions of citizen-centricity accordingly motivate this literature, with service state thinkers seeing digitalisation as a chance to dramatically

---

at the time. Indeed, several academics cited in this thesis actively protested against British identity cards. Researchers were influencing the laws around an emerging technology as it evolved—and this understandably brought a more normative edge to their writings as they critiqued contemporary systems that would likely affect their everyday lives.

re-imagine legacy aspects of government, upping the quality and quantity of the services offered to citizens, while also potentially personalising service delivery (JA Taylor *et al.*, 2009, p. 136). Once we become a truly digital society, a service state theorist would say, passports, driver's licenses, and utility bills will become a thing of the past—tools that are no longer fit for purpose. Ex-Prime Minister Tony Blair's tireless efforts to promote digital identity schemes typify this kind of thinking[15].

When it comes to service state perspective on digital identity, much of the existing work can be found in the outputs linked to the *Future of Identity in the Information Society* (FIDIS) project—a Network of Excellence which the EU funded for five years from 2004. FIDIS brought together practitioners and scholars across Europe to update much of the historical work on identification in light of the growing push in multiple states for digital systems (Rannenberg *et al.*, 2009). The network hosted a series of 'Identity in the Information Society' workshops, which spawned an academic journal of the same name. The journal was short-lived, with only seven issues published across three volumes, but remains the primary attempt to kick-start the study of digital identity as a concerted field beyond the confines of the far more critical surveillance and STS literatures. And, while the field never really caught on, the FIDIS outputs nevertheless remain a useful overview of the service state literature.

As the name implies, FIDIS can be loosely associated with the generally more optimistic 'information society' discourse that traces back to Manuel Castells (2009c, 2009b, 2009a) and Daniel Bell (1973)—though neither theorist focused on identity systems themselves. FIDIS was therefore defined by its relatively uncritical promotion of digital government goals and digitalisation[16]. For instance, only two of its seven deliverable streams ('Profiling' and 'Privacy and the legal-social content of identity') touched on remotely normative issues and, even then, the associated outputs are mostly descriptive and empirical in nature. These scholars thus primarily asked practical, technical questions surrounding the development and implementation of digital identity systems, rather than philosophically evaluative or prescriptive questions about the values such systems promote, or whether they should exist in the first place.

Take exemplary work from David Birch (2008). Birch is an identity practitioner and consultant, who provided a prescient appraisal of national identity cards in the

[15] Both during his time in Number 10 and more recently via his non-profit foundation, Blair has repeatedly pushed for biometric ID card adoption in the UK (BBC, 2005; Tony Blair Institute, 2019), championed digital ID-based international vaccine passports (A Bennett & Beverton-Palmer, 2020), and promoted digital identities as a solution for various global development challenges (Theodorou, 2022). Digital identity, in Blair's view, is an obvious piece of foundational infrastructure necessary for any modern, digital government—a view that many service state theorists share.

[16] Frank Webster's (2014) work provides a welcome critical counterpoint to this optimism, and links digitalisation to long running discourses around capitalist development.

journal's first issue. He discusses "using technology to deliver security and privacy in a new way" (Birch, 2008, p. 190), with reference to several nascent technologies ready to be deployed to deliver his vision of a smart biometric identity device. But while Birch's work is an interesting, high-level practical guide to building such a system, it plainly takes the need for a "modern identity scheme" as writ (Birch, 2008, p. 190). There is no deeper soul-searching, with his piece aimed squarely at policymakers already looking to deliver "a new identity ecosystem" that will "grow and flourish" once it is built using off-the-shelf technologies (Birch, 2008, p. 200). As with much service state literature, the basic need for a digital identity scheme is taken to be self-evident; the cornerstone of any good digital government strategy. And, as with many of other FIDIS outputs, values like privacy and security are advocated for—but from a technical, cybersecurity perspective, without any philosophical appreciation of their importance.

This lack of normative critique is surprisingly prevalent across the wider service state literature. As Taylor, Lips, and Organ noted, "research on e-Government largely ignores the [greater normativity of the] surveillance perspective, focussing instead on managerial issues of on-line service design and uptake" (JA Taylor *et al.*, 2009, p. 150). The exception is Lips (2009b, 2009a; 2010) herself, who has critiqued identity cards with various co-authors. This valuable work has covered topics including the citizen-state relationship, identity fixing, and public services improvement—which all bear relevance for my work. But, beyond Lips' work, the fact remains that much of this tranche of research bases "its analysis and prescriptive reasoning" on the opinions of 'on the ground' practitioners instead of any deeper philosophical evaluation of what is right, good, or just largely reflects the kinds of disciplines involved in the project (JA Taylor *et al.*, 2009, p. 136). The main field of scholarship involved in the FIDIS journal's first issue were the social sciences, law and legal philosophy, and technical research and development (Halperin & Backhouse, 2008, p. 82). And much the same is true of the more recent literature surrounding the concept of open-sourcing 'Government as a Platform' (GaaP), the spiritual successor to the service state view ("Government as a Platform in Practice," 2023; O'Reilly, 2011). All of these scholars are simply not trying to be normatively evaluative—and we should not fault them for this, though it does mean a lot of the work has limited import for an explicitly moral and political project like the one I am pursuing.

1.3 Limits of the Existing Debate

From the work outlined above, it is clear that a variety of important, normative questions readily arise from portions of the existing literature on national digital identity systems. Yet these are only partly, if at all, addressed by this work. Critiques advanced by sociologists, especially in the STS tradition, have indicated clear epistemological and political issues with state-deployed identity technologies that need resolving. The surveillance state literature goes slightly further, and has grounded resistance of what it sees as an unjustified surveillance tool. But this work

largely petered-out by the 2010s, and so is in need of an update for a modern setting. More recently, development scholars have lifted the torch, adapting many of the foregoing critiques to try and shed light on what is happening across much of the Global South. But this has limited salience for modern Britain—a country that is not developing nor deploying identity systems with no real predecessors, but rather wrestling with a long history with identification systems and mature administrative institutions. But beyond these issues in terms of timelines and appropriateness, allow me to briefly expand on three more, specific ways in which these existing literatures are lacking, before I extract some key themes to take forwards and address over the remainder of this thesis.

1.3.1 Turning Attention Home

Most importantly, although there is ample academic literature covering digital identity schemes in other countries, since the scrapping of identity cards there has been remarkably little written about British systems. After a flurry of activity around 2010 (D Barnard-Wills & Ashenden, 2010; Edwardes *et al.*, 2007; Aaron K Martin, 2012; EA Whitley & Hosein, 2010; Wills, 2008), in addition to the edited collections we have already discussed, only a handful of papers have since engaged with GOV.UK Verify, the successor scheme (Brandão *et al.*, 2015; Stalla-Bourdillon *et al.*, 2018; Tsakalakis *et al.*, 2016; E Whitley, 2016, 2018). Indeed, there is a complete lack of empirical, let alone normative, research considering Britain's modern identity schemes. Literature searches in mid-September, 2024, just before I submitted this thesis, for either "One Login" or "trust framework"—the names of the government's two current schemes—surfaced no results. Instead, the gap has been insufficiently filled by reports from think-tanks (Barnard, 2020; A Bennett, 2020; A Bennett & Beverton-Palmer, 2021; Nash & Smith, 2023) and trade bodies (Kiser, 2024; Marsman, 2024; OIX, 2021; Willars, 2019), as well as journalistic opinion pieces (Glick, 2020d, 2021c; Say, 2024). This is a significant oversight which this thesis consequently attempts to address. Not only is the British context interesting in its own right, but the country's chequered history with digital identity systems brings the normative contestation that has often driven policymaking to the fore.

1.3.2 The Limits of Privacy

Second, I must note that individual privacy rights are always the dominant critical tool deployed by surveillance state theorists (Lips *et al.*, 2009a, p. 718). Enjoying privacy is generally understood to mean having ''control of [one's own] personal information'' (Daniel J Solove, 2008, p. 24), or the ability to ''limit or restrict others from information about'' oneself (Tavani, 2008, p. 141). But, while other values may be mentioned, the crux of the problem always seems to be the increased informational awareness of the state—hence, the preoccupation with imagery of surveillance and

watching in identification contexts[17]. For our purposes, this is certainly useful. It links identification to philosophical accounts of surveillance which, as ethicist Shanon Vallor (2016, p. 188) notes, have enjoyed a long history of (political) philosophical attention ever since Plato. Some of this literature will thus certainly be helpful, and discussed momentarily. But privacy can also be a limiting lens. For instance, despite the range of issues they identify in the existing scholarship, Taylor, Lips and Organ (2009, p. 138) ultimately recommend bringing the surveillance and service state perspectives to bear on one another, deploying Helen Nissenbaum's (2004) notion of privacy as "contextual integrity". This no doubt captures some of the relevant concerns, but it will necessarily fail to account for all of the wider, interlinking normative issues at play. Privacy is just one value amongst many in a liberal democracy.

Along similar lines, historian Edward Higgs (2004, p. 18) has argued that a focus on privacy alone is too reductive, as any information gathering by the state is then seen as synonymous with surveillance and state control—with the only way to resolve these issues being greater privacy. If surveillance is the nail, privacy is the hammer. But this neglects both the implications of identification systems for other rights and values, as well as the potentially positive effects of state information gathering, which can help defend and strengthen various liberties and social goals. Health surveillance during the coronavirus outbreak, for instance, proved essential for saving lives (c.f., Lau *et al.*, 2021). Consequently, this is an insight I wish to carry forwards. While privacy is indeed a key value, making it, or any other value, the sole foundation of a critique leads to theory that overlooks the full breadth of considerations surrounding digital identity systems. A balance of values need to instead be carefully weighed and traded-off to ensure we avoid reductivism. Thus, my prior mentions of both liberty and equality, by way of discrimination, should signal that these values are also worth considering, and will be included in my analysis. Finally, we should not just be asking how society is changing along all these different axes, but also whether we want those changes and the society they will forge (Susskind, 2022, p. 260). This is where the normative aspect reasserts its relevance.

1.3.3 Beyond the State

Finally, contemporary British identity policy throws up a further issue for the surveillance state perspective. As I detail in *Chapter 6*, successive British governments have attempted to move away from purely state-based digital identity solutions. For the past decade, in fact, government has been trying to completely sidestep the notion of state digital identity provision entirely, instead favouring the creation of identity 'federations' amongst private sector identity providers operating on behalf of

[17] As Kevin MacNish (2017) has noted, while "trust, chilling effects, control, error and social sorting" are some of the further wrongs of surveillance that occasionally get mentioned, privacy is almost always the main complaint.

government (E Whitley, 2016). This metastisation of identity provision from government to corporations means that, in both public and private, citizens have become increasingly "governed by identity" (Amoore, 2008). This cements the technology as "a key mode of governance" in contemporary societies (CJ Bennett & Lyon, 2008, p. 3). But it is also not a unique phenomenon. The privatisation of identity provision can be seen as part of a centuries old trend of communication infrastructures—from semaphores, to telegraphs, phone lines, and the internet—being run as a private-public surveillance assemblage (Tréguer, 2019). This links to outsourcing conversations we will return to at length in later chapters.

So, what changes as a result? At the very least, the Big Brother-esque critiques advanced by surveillance state thinkers need to be revised to account for the private sector carrying out much (if not all) of the monitoring instead of government—as Oscar H. Gandy Jr. (1993) somewhat prophetically warned when he predicted that the 'panoptic sorting' of individuals would increasingly be managed by corporations, not states[18]. Additionally, as firms potentially gain power and insight through the popularisation of their digital identity systems, impetus emerges for considering how their monetisation of this position might affect society at large. Much academic attention has focused on Online Service Providers (OSPs) more generally (Kreiss & McGregor, 2018; Taddeo, 2019), but less studied are the often obscure corporations involved in the government's identity schemes. Finally, it might suggest that maintaining the traditional analytic public-private distinction has, in many ways, become unhelpful. In some contexts the distinction may even have collapsed, as both private companies and governments surveil the data we generate, as citizens and consumers (Barassi, 2019, p. 415). But this is primarily a problem for the surveillance state literature. Given their focus on citizen-centricity, service state thinkers do not necessarily care who provides public services so long as the service is effectively delivered. Privatisation is acceptable from the service state perspective, so long as the resulting service is adequately run for the citizen-consumer.

Regardless, the context in which a technology is deployed matters, and can considerably alter its socio-political implications. States are not companies and, despite the technical similarities, their digital identity systems are not normatively equivalent to corporate counterparts; they are inherently political, in terms of both their nature and effects. The translation of identity systems to governmental contexts thus requires careful consideration. Most obviously, governments possess unique responsibilities towards their citizens, residents, and visitors that businesses do not share. So, while companies might legitimately sell digital identity services to just a select few customers, it is usually thought that government should instead leverage the technology to improve all citizens' lives, via increased inclusion and better public

[18] Similarly, Taylor, Lips, and Organ (2009, p. 149) briefly recognise this "'blurring of public private boundaries' in service delivery" as a venue for future research.

services (McKenzie *et al.*, 2008, p. 3). As we have seen, justifications like these are the driving force behind some international development projects, yet many are still left behind. Sustained investigation of these blended or even wholly-privatised identity architectures is therefore required to see what effect they have. In particular, this must pay special attention to the market-driven mechanisms by which identification is now increasingly delivered. After all, market logics raise fundamental questions around the fair distribution of identities—tying access to digital identities to a profit motive for the first time in British history.

1.3.4 Towards a Holistic Solution

In sum, at least three lines of normative enquiry are beginning to present themselves. Namely, are we content with the impacts of digital identity systems for *liberty*, and its relation to citizenship, privacy, and other freedoms; *equality*, with regards to access and discrimination in both public and private contexts; and the role of *markets*, as a possible modifier to these two central pillars of any liberal theory? But behind all of this sits a recognition that making people visible to the state machinery through digital identity systems links our enquiry to decades of debate about state legibility and control. As we have seen, aspects of these essentially-political questions have been considered by other scholars. But, despite providing a valuable starting point, existing analyses are too limited. In particular, they are unconnected to an overarching theoretical framework. And none of this work has focused on the British case, despite its interesting history and unique systems. While discrete aspects of the problem have thus been analysed, no comprehensive pulling-together of the issues involved into a coherent whole has yet been achieved. This, though, is vital: many of these different aspects will likely conflict and so need careful balancing if they are to be fully resolved. To address these concerns, I will therefore now justify the value of reconsidering these questions holistically at the level of political theory, before introducing the liberal theoretical framework within which I will more fully analyse these interlinked normative considerations.

1.4 Political Philosophy

Political philosophy, or normative political theory, is concerned with the evaluation of concepts, values, and actions, as well as what ought to be done in light of them (Swift & White, 2008). Since the ancient Greeks, philosophers have considered the ethical problems that technologies can raise (Dusek, 2006). However, as Rosner (2014, p. 21a) notes, although "identity management research has been approached from legal, technical and sociological viewpoints […], [p]olitical science approaches […] are under-researched"—and, if political scientists are under-represented, then political *philosophers* are completely missing in action. As we will see, the analytic tradition has simply not engaged with digital identity systems in any meaningful way, and there are only limited implications we can draw from the continental tradition. But although this section shows that philosophers have paid national digital identity systems scant attention, there is plenty of parallel, normative research into socio-

technical systems and technologies of control deployed by states that we can use as inspiration to translate into this context. While much of this work is not directly relevant, it can nevertheless illustrate what stands to be gained from taking a political-philosophical approach to identity.

Perhaps most pertinent—and the only work directly engaging with the topic of digital identity systems from this perspective—is David Barnard-Wills' (2012) book-length "intervention in political theory" examining New Labour's identity card scheme. Barnard-Wills drew on a blend of Foucauldian and post-Marxist perspectives to understand British identity policy in the early-2000s through the lens of privacy and surveillance discourse. This is hugely valuable work, which has informed this project, but Barnard-Wills' study does only offer some glimmers of hope. First, it concerned a now-defunct identity scheme, leaving the last decade and a half of identity development in Britain unanalysed. Second, I have already discussed the limitations inherent in taking the privacy lens as foundational—we should also be considering these schemes in light of other values[19]. Finally, Barnard-Wills locates his work in the continental tradition, meaning we still lack a liberal critique of identity. What is more, his discursive focus is apt for unpicking the moral and political language used to sell identity cards, but reveals nothing about what a better alternative should look like. This accordingly gives us a place to start.

When it comes to other philosophical work focusing on identity systems, further contributions are few and far between—and almost all theorists have focused on ipse identity, not idem identity. Timothy R. D. Grayson (2003), for instance, self-published a rough philosophy of personal digital identity (rather than identity systems) over two decades ago. A few years later, P. J. A. de Hert (2008) defended the concept of a right to an online identity, again in the ipse sense. Ethicists have also explored some of the normative concerns around algorithmic systems constructing digital identities on our behalf (Manders-Huits, 2010), as well as the harms of profiling they can raise (de Vries, 2010). Likewise, Jeroen van den Hoven and John Weckert's (2008) edited collection on the moral philosophy of information technologies included a few chapters on personal identity, but is primarily only useful for showing how philosophical methods can shed light on problems at the intersection of technology, politics, and normativity. And, following this flurry of philosophical concern around digital identities through to the 2010s, interest has waned. All of these examples therefore fail to fully account for contemporary identity policy and practice, and specifically that which is managed by identity systems rather than performed by individuals on, for instance, social networking sites.

[19] A similar discussion of personal identity from the perspective of privacy alone falls into the same trap (Capurro *et al.*, 2013).

1.4.1 Lessons from the Philosophy of Technology

Although there is thus little directly-relevant political-philosophical fodder for an idem-focused study, there is nevertheless much useful philosophical work to consider. In particular, the large body of research under the philosophy of technology umbrella has always been concerned with evaluating technologies for monitoring and controlling populations (Vallor, 2022). As Sandra Barman (2006, p. 138) points out, "Rulers have kept records on the ruled since ancient times", via tools like the census and other "statistical representations". And philosophers have long taken note of this, connecting political technologies to the ability and power to rule. Politics is, after all, about who has the power to make decisions, shape others' choices, and decide who gets what (Lasswell, 1950). But the first step in making such decisions is knowing what you have power over in the first place. In Britain, the *Domesday Book* famously surveyed the population and their landholdings to facilitate revenue collection after the Norman conquest of 1066, directly connecting data collection to political power a millennium ago (Cobbe, 2018, p. 9). And it is easy enough to draw on normative critiques of these and subsequent practices to see how we might approach identity systems today.

What, then, can philosophers of technology tell us about systems of control? Here, another short work of continental philosophy points us in the right direction. Gilles Deleuze's incredibly brief but prescient *Postscript on the Societies of Control* warned that "electronic cards" may provide us with access one day before rejecting us the next thanks to the inscrutable demands of computerised tracking systems (Deleuze, 1992, p. 7). The very language of control, Deleuze wrote, was becoming comprised of the "codes" and "passwords" that "mark access to information" (Deleuze, 1992, p. 5). In recognising the growing importance of computerised access control systems all the way back in 1992, Deleuze extended Foucault's (1991) perennially-popular characterisation of surveillance as a form of disciplinary technique. Today, Foucault's work remains favoured amongst surveillance theorists, who see modern, data-based techniques for controlling populations as an extension of nineteenth century obsessions with measurements and observation, particularly with regards to modifying behaviour (Barry, 2020, p. 2). As we have already covered, the panopticon is the example par excellence here—a system of surveillance and control built upon the threat of constant observation by agents of the state, long before digital technologies could super-change the threat via unblinking eyes. And certain kinds of identity systems will no doubt raise similar concerns.

More generally, several recent works have mounted normative arguments against digital surveillance and its disciplinary uses. Kevin Macnish (2017) has been a pioneer in this space, connecting sociological criticism of surveillance systems to classical philosophical views about privacy. Since then, with Adam Henschke, he has also co-edited a collection applying the ethics of surveillance to the coronavirus crisis and the enhanced surveillance it brought with it (Macnish & Henschke, 2023). Although this

does not touch specifically on identity systems, it is not hard to see a connection. The past few years have also seen theorists at the bleeding-edge propose a variety of new digital rights to cope with algorithmic profiling (De Gregorio, 2022; Wachter, 2019; Wachter & Mittelstadt, 2019), as well as ethical principles oriented towards similar ends (Coeckelbergh, 2018; Floridi *et al.*, 2018). This might likewise provide some guidance as to how to address the harms of identity systems.

Yet, as we have discussed, the focus on privacy and surveillance can overlook other liberal values. Carissa Veliz's (2021) *Privacy is Power* is therefore a particularly valuable addition, as it suggests practical steps individuals can take to try and resist corporate surveillance of their personal data. Véliz is one of the few theorists to have gone beyond privacy alone to consider the impacts of corporate surveillance for both individual and collective power. Other similar contributions are Faridun Sattarov's (2019) more general exploration of power and technology, as well as Henrik Saag Saetra's (2021), book-length treatment on liberty under Big Data. Both provide welcome case studies in tying modern digital systems to specific freedoms in a liberal society. Beyond these, Mark Coeckelbergh (2022) has presented the first monograph on the political philosophy of artificial intelligence. He has thus connected digital technologies to not only privacy and liberty, but also equality, democracy, and justice. And, in the popular press, Susskind has recently put forward a political theory of digital government (2020) and regulation (2022), both built on neo-republican (rather than liberal) foundations.

As this short survey demonstrates, political-philosophical engagements with important digital developments are still embryonic. Yet, in all these cases, direct engagement with cutting-edge empirical research has allowed scholars to produce exciting, non-ideal theory. These latter contributions, in particular, therefore present a model for constructing an overarching normative theory to help understand and respond to digital systems of control, intertwining a philosophy of technology with political-philosophical suggestions. None, however, have discussed identity systems. This is consequently very much the kind of work that I seek to emulate, albeit in a specifically-liberal mode, and newly-focused on digital identity systems and their various interrelated moral and political impacts. All that remains is for me to sketch the liberal approach I will be taking on to achieve these ends over the course of this thesis.

1.5 A Broadly-Liberal Theoretical Framework

There is a more fundamental reason to pursue a political-theoretical approach. Much philosophy of technology is individualistic, and so can readily elide the societal angle—indeed, popular "political theory from the English-speaking world, such as work by Rawls, Sandel, Walzer, MacIntyre, or Nussbaum is often not even mentioned, let alone used, within contemporary philosophy of technology" (Coeckelbergh, 2018, p. 5). This strikes me as a significant shortcoming. Especially in the case we are discussing, the role of the state and its mediation between individuals is essential. This

firmly locates a critique of British digital identity systems within a basic liberal-theoretical context, and demands a political angle to any analysis. We must, therefore, go beyond the philosophy of technology over the remainder of this chapter. This starts with consideration of freedom—or liberty—and its relation to the state via the notion of citizenship. I then turn to the other key liberal value of equality. This is because liberty and equality, and especially the nature of their interrelation, are centrally important considerations for any liberal theory (Duncan Bell, 2014). Finally, we must also bear in mind that contemporary Britain grew out of the postwar welfare state. The Thatcherite valorisation of markets and privatisation that this eventually gave way to will therefore also be relevant for our enquiry—though, we will cover the historical account in far more detail in later chapters.

1.5.1 Liberty and Rights

The most common way to divide different species of liberal theory up is by distinguishing 'classical' from 'social' liberalisms (Duncan Bell, 2014, p. 684). This captures the sense in which liberal freedom has evolved over the past few centuries. Liberals traditionally understood liberty in primarily 'negative' terms; synonymous with the degree of freedom *from* coercion, obstruction, and interference at the hands of others which an individual enjoys (Berlin, 2002, p. 170). A commitment to negative liberty holds that I should, for instance, be able to choose how to live without someone else dictating what I can say, what happens to my property, or which religious or political groups I belong to. The more autonomy I enjoy in these respects, the more freedom I might be said to have—and this grants me the space to live my life according to my own understanding of what a good life should be. Taking the position to its libertarian extreme, I might be thought of as completely free if I was never subjected to any external obstacles or barriers to exercising my will. Classical liberals might accordingly find prima facie issues with any systems or laws that restrict access to essential freedoms—for instance, political rights via the introduction of, say, voter ID requirements. Overly onerous requirements to identify oneself to election clerks, could represent a clear obstruction to liberty in this sense.

However, a more 'positive' conception of liberty is today favoured by many liberal theorists[20] (e.g., Raz, 2009). This pays closer attention to whether I have the freedom *to* act in a particular manner, and can be parsed in one of two ways. The first concerns a psychological sense of self-realisation (C Taylor, 1985, p. 212). Because each citizen is generally left to pursue their own ends under liberalism, some theorists maintain that those ends cannot be the result of "lack of awareness, or false consciousness, or repression" (C Taylor, 1985, p. 212). Yet other accounts go beyond

[20] While Rawls (2005, pp. 201–203) explicitly tried to sidestep this positive/negative distinction, emphasising the complex web of rights and duties which condition a person's freedoms, he generally discusses the package of liberties an individual can expect the state to provide and protect negatively, in terms of freedom from outside "constraints" and "interference".

psychological constraints alone. Following R. H. Tawney, theorists like Amartya Sen (1985) hold that any measure of freedom must also seriously consider an individual's *ability* to exercise their own autonomy. This may be straightforwardly constrained by external interference, but also a lack of access to vital resources such as money or an education. In the case of voter ID, we might consequently consider the cost of acquiring sufficient identification as well as any accessibility issues, beyond simply whether or not an election clerk is obstructing us. Do appropriate alternatives exist for eligible voters who cannot afford to pay? And what about people that might find it difficult to apply for sufficient identification due to disability or illness? More fundamentally, as identity systems are often used to manage access to state goods, an immediate potential conflict arises on the positive account, too.

In general, though, we can say that the liberal project—whichever conception of liberty you favour—attempts to maximise each individual's liberty under a democratic framework whereby all individuals can achieve maximal liberty together (Duncan Bell, 2014, p. 694). Of central concern for liberal theorists is therefore the question of the nature and extent of any one individual's liberty and its relation to that of other citizens. Society, after all, comprises a collection of individual citizens. And each of these citizens might, in exercising their liberty, encroach on the liberty of another. Yet, as the voter ID example demonstrates, what makes adjudicating between competing citizens' claims to freedom challenging is that liberty of either flavour is difficult to analyse in the abstract. While it is obviously true that being imprisoned reduces my liberty—imposing a significant obstacle to my freedom and constraining my will—it is much harder to say how precisely voter ID laws will affect me. This is because, in reality, liberty is not a monolithic, abstract concern; it can be better understood as a kaleidoscope of more specific freedoms and rights (Carter, 1995). This is an insight we will need to take forwards, looking at how to balance the various values and freedoms involved in the construction and administration of identity systems.

1.5.2 Citizenship

This brings us to another central concern for liberals: the nature of citizenship. Liberty, the state, and individuals are intimately bound up in liberal and neoliberal theory (Voinea *et al.*, 2023). In particular, it has long been understood that the citizen chooses to give up some of their freedoms in return for the mutual protection of government in a community of equals underwritten by the social contract (Locke, 1988). And, precisely because liberties are complex and multifarious, and different people value different freedoms, most liberals recognise that competing freedoms need to be balanced, often with assistance from the state, in order for a stable society to exist (Crowder, 1998). A solution is therefore required which can a) adjudicate between different claims to liberty and interference, as well as b) provide means for individuals to work together where individual liberty is insufficient to achieve some

common goal. In other words, individuals must come together to create a state and agree to share in the mutual benefits offered by its citizenship.

Thus, a tension between the needs of the citizen and society as a whole is immediately embedded within a liberal understanding of the world. We might think of the Chinese social credit system, where social scoring is said to benefit society at large, even if limits the freedoms of certain individuals (Orgad & Reijers, 2021). And much the same can be said of other identity systems, given their fundamental orientation towards discrimination and control. When is it acceptable to use identity systems to pursue the betterment of society at the cost of individual liberty? However, as Julie Cohen (2012) has argued "liberal and neoliberal theories of citizenship tend to be relatively insensitive to questions of sociotechnical configuration", despite the importance that technological systems increasingly have for understanding the citizen-state relationship. This is a significant oversight. As Miriam Lips (2013, p. 61) has noted, digital identity systems fundamentally alter how the state manages and interacts with its citizens, changing both "the meaning of citizenship" and the relationship between the citizen and their state. But this means that identity is now centrally important for the study of modern digital governments (JA Taylor *et al.*, 2009, p. 137), particularly as governmental digitisation continues to progress. But liberal theory will need extending to accommodate this insight.

Regardless, a key takeaway is that digital identity systems have the potential to greatly expand, but also constrain, citizens' freedoms. I have already discussed how better and more convenient access to robust public services could improve citizens' lives (McKenzie *et al.*, 2008, p. 3). On a more positive, capabilities-sensitive account, this is especially clear. Identity systems are also crucial for modern policing, helping to secure borders, combat identity theft and reduce financial crime (CJ Bennett & Lyon, 2008, p. 5). In this way, they assist in protecting individuals from harm, whilst allowing them to enjoy various other important freedoms (Higgs, 2004, p. 192). All of this could help to ensure a basic level of liberty in a society, protecting the social contract. But, at the same time, we have also seen how such systems can be tools for surveillance and exclusion—preventing people from accessing these very same goods and liberties, should they fall foul of the authorities or fail to submit to registration. And the normative stakes are especially high in governmental contexts. Asymmetries of power mean that governments can threaten anything from reduced access to state resources and services to "fines, penalties, or imprisonment" for noncompliance with registration efforts [21] (Watner, 2004, p. 250). Thankfully, however, political philosophers are attuned to asking who counts as a citizen (c.f. Carens, 2013), even if little work has considered the technical systems increasingly used to answer these

[21] During the coronavirus outbreak, for instance, freedoms of association and movement were made contingent upon globally-recognised digital vaccine status records, tied to identities (Ada Lovelace Institute, 2021). Handing such "instruments of almost limitless capacity" to elites can thus only be done with full understanding of the precarity involved (Higgs, 2004, p. 193).

questions. Exploring the changing nature of citizenship, as modified by digital identity systems, will thus be vital as we move forwards.

1.5.3 Equality and Justice

If adequate identification is increasingly a necessary precursor for proving one's status as a citizen, then this immediately raises equality-related questions around access to liberties and goods, as well as possibly the fair distribution of identities themselves. However, liberals have always struggled to agree on what precisely 'equality' means, and what should be equalised (Sen, 1995; Young, 2001). For centuries, liberals of most stripes have come to some consensus on the fundamental equality of humanity—i.e. that all humans are deserving of the same basic dignity and respect due to their status as humans (Waldron, 2017). This tells us little about distributional issues regarding the meting-out of material goods, though. What precisely should be equalised? Few, if any, argue for the simple, flat distribution of a country's material goods amongst the population, so is it the opportunity to earn that we should instead be striving to make consistent? Or is it the outcomes of our work that should be made equal, regardless of the opportunities we may or may not have had? Perhaps, instead, it is better to equalise individual interests or welfare rather than opportunities or material outcomes? Or is it equal capabilities to live and act, as outlined by Sen, that are important? The criteria for equality under liberalism are demonstrably multiple and highly contested.

These debates are relevant to us for two reasons. First, there is the inherently discriminatory nature of digital identity systems. Identities define who is and who is not allowed access and granted entitlement, which links them directly to questions around equality of opportunity as well as interest and welfare. As we cover in *PART II*, everything from jobs to housing and benefits have been made contingent upon identification in Britain, via policies like DBS checks, Right to Work, Right to Rent, and Universal Credit (DSIT, 2024b). Any of these systems can thus engender unjust exclusion and discrimination, though we must also pay attention to when and how people might be legitimately excluded. In particular, digital identity systems can easily risk people's lack of technical literacy, connectivity, and acceptance of digital technologies undermining equality and justice for the less technically-savvy—especially if access to public services becomes contingent upon digital identification. At the very least, liberal governments might attempt to ensure that access to state services never becomes solely dependent upon submitting to digital systems. Providing alternative, non-digital routes for interfacing with the state could be one way to ensure that those who cannot, or will not, adopt digital identities are not disadvantaged as a result. But this will need to be defended.

Second, if digital identities can properly be conceived of as something analogous to 'things' that can be held and presented, bought and paid for, then distributional questions are also unavoidable. Should the ability to prove our identity be conceived of as a good, service, or commodity that we purchase? How far, if at all, should

identification be subsidised for those that cannot pay? And does buying an identity from the marketplace, versus being given one by the state, alter the value of that identity? For instance, making international travel contingent upon purchasing a passport might well be exclusionary for those who cannot afford to pay, but this could be a price worth paying for adequate border security and the autonomy that safe and free international movement enables for those who can. The question then arises: to what extent it is justified to expect people to pay to exercise their rights to free association?

These are big questions. As they illustrate, however, one of the strengths of the liberal approach is that it takes these conflicts seriously, paying attention to the theoretical and practical work required to weigh competing demands. Although important, liberty is not the "sole criterion of public action", which is why liberals throughout the nineteenth and twentieth centuries worked to create institutions that could accommodate and promote a range of potentially incommensurable values and freedoms, including equality (Galston, 1999, p. 769). And the upshot is that such attention to 'value pluralism' provides a rich conceptual tapestry for the liberal political theorist to draw on when critiquing potentially unjust arrangements, moving far beyond a narrow focus on, say, privacy or freedom alone (Crowder, 1998). This will be hugely important for the rest of this thesis.

1.5.4 Marketisation

Markets have a difficult relationship with liberalism. In the pursuit of liberty, liberals have generally countenanced the market as a tool for enabling efficient economic exchanges (Wolff, 2011, p. 171). Some have even gone so far as to suggest markets are the best way to facilitate the efficient usage of knowledge across the entirety of society, making them far preferable as a means of social coordination to central planning by governments (Hayek, 1948). But, recalling the liberal versus social distinction I made earlier, some more socially-minded liberals have worried that unconstrained markets can have unacceptable effects for society at large (Posner & Weyl, 2018). Indeed, philosopher Michael Sandel has called marketisation—the proliferation of market-oriented logics into spheres of life that were previously not driven by such norms—"one of the most significant developments of our time" (Sandel, 2012, p. 7). Since Thatcher, across much of the world markets have become the default tool for allocating any number of social goods via the 'neoliberal' ideas of the New Right—and this is directly reflected in the move to federated identity systems in Britain. Marketplaces for identity were construed as a more efficient and privacy-preserving model than a centrally-run, governmental system. But, as we will see, the result was not very successful for inclusion.

Beyond inclusion worries, neoliberal enthusiasm for markets has also been accused of casting political issues in narrowly economic terms, which critics argue even risks "quietly undoing basic elements of democracy" (W Brown, 2015, p. 17). Such economisation is taken to be particularly damaging when the "crass

commodification" of spheres not previously ruled by market logics leads to human exploitation or limited access to important democratic goods (W Brown, 2015, p. 29). And, in particular, recasting citizens as neoliberal consumers could be construed to reduce the democratic subject to a mere market actor (W Brown, 2015, p. 31). To what extent aspects of recent British digital identity policy can therefore be cast as neoliberal intrusions into the liberal democratic welfare state, and what implications for citizenship this might have, will therefore be a key question in this project. First, it will be interesting to see just how coherent a move towards federation is from within a neoliberal perspective, if indeed a neoliberal approach to government modernisation has driven recent British developments. But we will also need to explore whether economisation is consistent with a commitment to liberal democratic principles and a liberal notion of citizenship. Nonetheless, liberalism provides key normative tools for evaluating the changing nature of citizenship under neoliberal logics and the introduction of identity systems more generally.

1.5 Summary and Next Steps

This chapter has reviewed what we currently know about digital identity systems, with a focus on the moral and political aspects of such systems. It has become clear that digital identity systems raise a range of complex and potentially-conflicting normative concerns. Consider such systems from the point of view of the individual and society at large. At the individual level, digital identities are becoming essential for the exercise of liberty, both online and offline, in many situations. But how does identification affect freedom? And what choices should we have over submitting to such systems? Relatedly, the importance of identity systems for inclusion raises unavoidable questions of justice and dessert. Who should have access to identities? What protections should those who do not (or cannot) want to use them them receive? And how can we exercise our rights around identity, if such rights even exist? Finally, at the societal level, we must consider questions of responsibility and power. What should the digitally-mediated relationship between the citizen and the state look like? Who should manage the state's identity systems? And how can we ensure that the power digital identification gives powerful institutions over individuals is not abused?

As I have shown, however, these interlinked issues have so far only been analysed in relative isolation from one another, and not from a unifying, political-philosophical perspective. Some questions, particularly relating to the harms of surveillance, are at least partly addressed in prior research. But while there are strong descriptive accounts of historical identification systems, for instance, we lack both normative evaluation of previous British systems and up-to-date analysis of the contemporary British context. Likewise, it is only with regards to the foreign case studies mentioned above that some more political questions have been asked—but not by political-philosophers. A vital piece of the puzzle focusing on British policy is therefore missing, and specifically from a liberal-theoretical perspective. But the upshot of this is that it gives me plenty to consider—particularly in terms of the need to uncover more details

about the British context through interviews with experts well-placed to shed light on such questions. After all, as Adam Swift and Stuart White (2008, p. 49) have argued, it is only "by combining value judgements with relevant and appropriately detailed empirical social science [that one can] ordinarily work out what policies should be urged in any particular context".

The deeper problem, however, is that existing attempts to answer these questions have dealt with the issues in an altogether inadequate, piecemeal way. Social scientists, legal theorists, and a few philosophers of technology have looked at aspects of digital identification technologies through the lens of specific moral and political values, but in a narrow manner which fails to account for how they might fit into a wider liberal-democratic theory of digital identity. This chapter has therefore begun to illustrate what stands to be gained from bringing a holistic, political-philosophical approach to bear on these issues. As Coeckelbergh (2018, p. 6) summarises, the discipline "offers excellent resources for thinking about justice, equality, freedom, democracy, and other political principles which, unfortunately, are not often used by philosophers of technology to discuss the societal impact of technology." Indeed, as I argue in the next chapter, making an informed assessment of the various normative challenges highlighted above is exceedingly difficult without an overarching framework fit for balancing various competing concerns. The rationale for this project should accordingly be clear, and it is to the specific methods by which I will achieve this balancing that the next chapter consequently turns.

Chapter 3.

Methods and Research Design

As we have seen, the digital identity-related policy decisions facing Britain are shot-through with concepts that need clarifying, values that must be weighed and balanced, and courses of action that require normative justification. Yet the dearth in political-philosophical research engaging with the topic has left a normative gap in the identity landscape. There is, then, philosophical work to be done here. But discussing how to go about doing that work—especially in a thesis not focused on philosophical methodology—is relatively unusual. Historically-speaking, political philosophers have rarely provided formal explanations of their methods (Leopold & Stears, 2008, p. 1). Even including a dedicated methodology chapter, like this, is uncommon. Nonetheless, the twenty-first century has brought with it rising interest in how political philosophers theorise and what, in doing so, we hope to achieve. This chapter can accordingly be read as my contribution towards greater methodological transparency. It specifies the methods I used to put theory to work in this project, and details how I integrated normatively-relevant aspects of British digital identity systems with an understanding of the contemporary policy landscape.

In particular, I first argue that my theorising had to eschew the extremes of both top-down and bottom-up methodologies. This allowed me to pursue the creation of empirically-informed, grounded theory that nevertheless retained the action-guiding power of idealisation. I then elaborate why the method of reflective equilibrium (RE) was best suited to realising this approach. After outlining the methodology in general terms, I specify the public flavour of 'wide' RE I used in this project. Deviating slightly from the status quo, I argue that the benefits of incorporating others into the RE process—by carrying out qualitative interviews—are hard to deny. This allows the theorist to introduce novel insights to their position, adding theoretical and practical detail to their existing thinking while also helping surface biases and misunderstandings. Moving on to discuss my particular research design in the second half of the chapter, I then justify two key decisions: scoping the study to British digital identity systems, and the use of digital interviewing techniques to integrate expert insights into my equilibrium. Altogether, I explain how this empowered me to weave a cohesive and empirically-sensitive theoretical scaffold around the British digital identity context, building a strong base for the theorising to come in later chapters.

3.1 Politically-Engaged Theorising

There are real questions surrounding the relationship between politics and philosophy. Over the course of the twentieth century, many philosophers at institutions like Oxford effectively retreated from the frontlines of politics, instead pursuing "logical rigour, terminological precision, and clear exposition" in heavily abstracted and idealised arguments (List & Valentini, 2016, p. 525). Indeed, much of this work ultimately became so far removed from the realities of governing a country that it had "little immediate or concrete significance for policy" (Swift & White, 2008, p. 52). This kind of philosophy's utility for guiding both public debate and policymakers was consequently neutered. As Jonathan Wolff (2018, p. 13) has suggested, "[t]he options for a political philosopher were to defend or attack an existing grand theory, or, in a daunting flight of fancy, attempt to construct a new one". Yet for many, myself included, this turn towards abstract analyticity in the twentieth century was entirely undesirable. Even the best-crafted concepts, principles, and theories need to correspond to something 'out there' in the world to be useful (List & Valentini, 2016, p. 544). I consequently agree with Adam Swift and Stuart White (2008, p. 50) that, given political action's inherently value-laden nature, political theory has a natural role to play in guiding policy decisions. One of my ambitions with this project was therefore to generate the kind of theory that could achieve such an end.

However, simply seeing political philosophy as 'applied ethics' does not get us very far. On such 'top-down' views, theorists merely project their ready-at-hand theories onto concrete cases (Doorn & Taebi, 2018, p. 491). The problem is that, with a few exceptions, these grand theories—ahistorical and free-floating like mathematical proofs—remain so abstracted from the complexities of everyday life that they are of little practical value to people who find themselves embedded in historically-conditioned contexts of power, domination, and injustice (Brandstedt & Brännmark, 2020, p. 356). A victim of identity theft, for instance, will struggle to find the general concept of liberty or harm useful for their assisting with their predicament. For action-guiding purposes, this model is thus equally unworkable. It leaves the political philosopher with little more to do than examine, clarify, and catalogue the different concepts and values (and their trade-offs) at work in any particular case, making it hard to make "principled recommendations for how such things ought to be done" (Floyd, 2017, p. 368). Like a doctor diagnosing ailments without prescribing correctives, it is hard to see the point. Theory is reduced to "providing the 'philosophical foundations' for social and public policy", but cannot offer any real guidance when it comes to the knotty problems faced by policymakers (Wolff, 2011, p. 14).

Yet the other extreme is just as lacking. The most committed 'bottom-up' approaches—which narrowly concern themselves with only the concrete here and now of situations—run the risk of focusing too much on the "particularities of the

specific case […] without any reference to ethical theory or principles" (Doorn & Taebi, 2018, p. 491). It is true that, on their own, the details of an identity theft will not help us much with uncovering the general normative rules at play in identification, or the policy recommendations that might flow from them. Such details might be sufficiently action-guiding for the specific situation but, due to that specificity, we lose the useful ability to generalise. Additionally, in cases of disagreement between the various parties involved, a reductively bottom-up approach cedes the possibility of drawing on wider, shared theoretical apparatuses that could help justify mutually-acceptable courses of action (Doorn & Taebi, 2018, p. 491). Stakeholders with conflicting views will therefore be harder to reconcile, as appealing to common ground at higher levels of abstraction (the meso-levels of principle or theory) cannot be done. But there is much to be said for a bottom-up view that is not quite so militant. Indeed, attempting to address the complexities of digital identity systems in Britain without understanding the unique context in which the country finds itself would likely be just as challenging as trying to reason from abstract first principles.

As a result, some have begun to pursue what Wolff (2018) terms a more *engaged* way forwards. Following the so-called 'empirical turn', many philosophers now recognise data to be a "constitutive aspect of their arguments and theorizing" (Perez, 2020, p. 339). Amatrya Sen's (1983, 1999) pioneering work, which paid close attention to how political and economic systems actually affect people's lives, perhaps best exemplifies this kind of approach. While Sen and others would admit the theorist's job has always been to "clarify arguments and to highlight the values involved in political choices", they would also emphasise that theory should "be supported by social science research to specify the real-world conditions and consequences of the choices that its normative propositions advocate" (Bauböck, 2008, p. 40). This is an approach that has found particular traction amongst philosophers of technology. While recognising that "[i]t is necessary to measure the results of bottom-up investigations […] against critical standards of independent moral principles" (Brandstedt & Brännmark, 2020, p. 356), such theorists also seek to ensure that appropriate attention is "paid to contingency and the social constructedness of technology" to avoid the limited import of top-down prescriptions (Doorn & Taebi, 2018, p. 489). My task in this thesis thus became clear: to balance relevant, descriptive content about the case at hand, surfaced from below, with the requirements of any normative theories exerting structural pressure from above.

In practice, this would mean using empirical data to more tightly integrate my theory development with prevailing political and institutional realities (de-Shalit, 2009, p. 42). This was, of course, easy to say, but somewhat harder to realise. What role would data need to play in surfacing descriptive insights? And how, precisely, could different perspectives be integrated? As we will see, the key issues around identity could certainly be aggregated from people already well-placed to shed light on those problems. This helped account for the 'non-ideal' nature of political reality, ensuring that the "morally relevant" experiences of experts and practitioners could be

incorporated into my bottom-up theorising (Widdershoven, 2007, p. 49). But this should not be taken to suggest that empirical data supplanted normative theorising in this thesis. Such a move would have collapsed philosophy into the social sciences, running the risk of generating oughts from what is. Instead, the approach I took is best understood as one of many recent attempts to show how greater sensitivity to concrete realities can make normative theory "more attentive, precise and reliable" (Perez, 2020, p. 343). Following Avner de-Shalit (2009, p. 43), the aim was to once again make theorising a politically-engaged act of democracy rather than a narrowly academic pursuit—to put the 'political' back into political philosophy. And by far the most developed methodology for achieving such empirical sensitivity, through a blended top-down/bottom-up approach, is reflective equilibrium.

3.2 Reflective Equilibrium

Popularised by John Rawls (1951, 1974, 2005), and so forever guaranteeing its favour amongst liberal theorists, RE is the leading methodological approach in contemporary political theory (List & Valentini, 2016, p. 542). Indeed, it is sometimes considered "the" method of philosophy *tout cour* (Lewis, 1983, p. x), with particular recent "scholarly precedent" surrounding its use in the practice-orientated fields of technology ethics and bioethics (Hoffmann, 2017, p. 1601). Much of the method's popularity stems from the fact that RE strikes "the desired balance between practical relevance and thorough criticism" that many deem necessary for doing "practical ethics" (Brandstedt & Brännmark, 2020, p. 357). Norman Daniels (1996), for instance, has powerfully demonstrated RE's value in this regard. He has repeatedly employed the method to solve complex, multi-stakeholder, problem-driven political issues, such as during a public consultation for President Clinton's health-care reforms in the United States (Brock & Daniels, 1994). To me, this cemented RE's utility for this project. To further defend its value, however, I will now sketch the basic method before demonstrating how my preferred flavour of RE—which incorporated elite interviews into the theory construction process—was particularly well-suited to realising the engaged kind of theorising outlined above.

The basic aim for the normative[22] theorist carrying out RE is to bring their "considered judgements" about a situation into a holistic state of coherence with a set of principles they develop to systematise those judgements (Rawls, 1974, p. 8). This is how Rawls (1974, p. 289) summarises the process:

> People have considered judgments at all levels of generality, from those about particular situations and institutions up through broad standards and first principles to formal and abstract conditions on moral conceptions. One tries to see how people would fit their various convictions into one coherent scheme, each

[22] Although my focus here is normative, RE has been successfully applied in other contexts. See, e.g., Elgin (1999) and Lewis (1983).

> considered judgment whatever its level having a certain initial credibility. By dropping and revising some, by reformulating and expanding others, one supposes that a systematic organization can be found. Although in order to get started various judgments are viewed as firm enough to be taken provisionally as fixed points, there are no judgments on any level of generality that are in principle immune to revision.

Even from this short passage, we can extract several key points about RE. The first is the breadth of Rawls's initial inputs. The second is his lack of epistemic commitment to these inputs. And the third is the process's iterative nature. To begin with, Rawls's summary makes the method's inclusivity immediately apparent. Considered judgements are those convictions we continue to hold under conditions well-suited to deliberation[23] (Knight, 2017, p. 47). Because these judgements, or initial inputs, amount to all the theorist's firmly held beliefs about a topic at multiple levels of abstraction—from the particular up to the general—relevant insights from theory and practice are consequently priced-in from the outset. For instance, universal commitments like 'privacy is an important liberal value' might sit alongside more concrete judgements like 'centralised identity registers always lead to unwarranted surveillance'. Built into RE's very fabric, then, is an appreciation of both the normative and empirical contexts surrounding a situation.

Secondly, note Rawls's lack of commitment to his starting points. Although there is some "initial credibility" given to the considered judgements and emerging principles, no single element is "immune to revision" (1974, p. 289). RE's starting points are no more than that. While we might complete the theorising process mere inches from where we began, we cannot rule out vast evolutions in our thinking ahead of time—even if it would upend our existing commitment to a well-established theory, principle, or judgement. After all, manoeuvring towards preordained outcomes would mean engaging in motivated reasoning, not open-minded theorising. Much of RE's appeal thus stems from this holistic approach to developing a position: beyond simply including normative and empirical content, it explicitly encourages theorists to deeply analyse moral and political issues from the top-down and bottom-up perspectives simultaneously (Doorn & Taebi, 2018, p. 491). RE thus facilitates "real dialogue between theory and practice by not assigning a preferential status to either of them" (De Vries & Van Leeuwen, 2009, p. 491). We must take part, in other words, in a properly grown-up evaluation of the full complexities of an issue, and are made to make precisely the kinds of trade-offs we often see in live policy discussions.

The third and final aspect of RE we can extract from the passage above is the method's iterativity. Making progress by following a justifiable and deliberative procedure is what matters to Rawls, regardless of our initial commitments (Walden,

[23] In other words, when not overly tired, under the influence of alcohol or drugs, pressured by other individuals, etc.

2013, p. 245). Actually reaching an equilibrium—the process's end state—therefore involves the theorist carrying out a procedure of repeated comparison and revision, "resolving inconsistencies" along the way until all the various elements "provide mutual support to each other" at all levels of abstraction (Tersman, 2018, p. 1). This is a highly cyclical process[24]. In finding the combination of elements that best support one another, the theorist must begin by developing a candidate apparatus of principles to systematise and rationalise their initial set of considered judgements. Then, on further inspection, wherever conflicts are identified, a process of "mutual adjustment" is carried out (Rawls, 2005, p. 20)—a mechanism borrowed from Nelson Goodman (1955). Effectively, the theorist repeatedly adjusts their judgements and principles as necessary to resolve any contradictions. After a sufficient number of these revisions, Rawls tells us, a coherent whole will eventually take shape, with all the various elements deriving reciprocal support from one another. This is the eponymous state of reflective equilibrium, which forms a theoretical scaffold for further moral and political decision making (List & Valentini, 2016, p. 526).

3.2.1 Narrow Versus Wide Equilibria

If successful, the theorist will now possess a set of moral and political principles, generated from their considered judgements, then refined and balanced through a series of mutual revisions. But what properties does this set of beliefs possess? We call it a) an equilibrium because the various elements in the end state offer each other mutual support and fully cohere, and b) reflective because the theorist has adjusted the elements without prejudice to weed out conflicts (Doorn & Taebi, 2018, p. 492). Unlike with more traditional, foundationalist approaches to political and ethical theorising, RE therefore draws its strength from from "the mutual support of many considerations, of everything fitting together" (Rawls, 2005, p. 21). Locally, individual principles and judgements will support one another more or less directly, while, globally, clusters of these elements will provide holistic support by consistently interlocking with one another. The whole can accordingly be thought of as a spider-web of intermeshed beliefs. And, to be clear, although the foregoing might have suggested that clear distinctions exist between the various elements in an RE, this is

[24] The method is therefore time intensive, but an upshot is that this cyclicality deflates the charge of conservatism commonly levelled against RE. The worry is that RE merely systematises, dogmatically, whatever biases we might already hold by taking our considered judgements as its starting point (Floyd, 2017, p. 377). But any reasoning needs to begin somewhere, and where else than with what we already think? The challenge to the critic, which remains unanswered in the literature, is to present a credible alternative starting point (Pogge, 2007, p. 176). The plain truth is that theorising that does not include at least some of our existing beliefs is impossible. Contra conservatism, then, Rawls's stipulation that any of our beliefs must in principle be open to revision actually points the way towards progress and away from dogmatism and bias (van der Burg & van Willigenburg, 1998, p. 10). Although finding an equilibrium simply must start from the examination of judgements a theorist already holds, these are never taken to be foundational. They are merely the epistemically available starting points we have to build from, always themselves open to revision.

not really the case. The line between judgements and principles is only analytical. As Carl Knight clarifies (2017, p. 53), it is no more than "a familiar and often helpful way of arranging our thoughts"—but "there is no problem with the boundaries between [the different elements] being fuzzy or overlapping" in practice.

There are several advantages to this coherentism. The first is that it "recognize[s] the fallible and provisionary nature of moral judgement" (van de Poel, 2016, p. 188). Not only do the bounds of normative acceptability change over time but, with hindsight, it often turns out that we were wrong. RE accommodates this, explicitly allowing for revision in light of new information. And, in the fast-moving, technical debates this project enters into, refusing to ossify any foundational beliefs that may later have turned out to be misguided was highly advantageous. The second benefit was that coherentism allowed me to leave certain controversial meta-beliefs unspecified. RE "leaves open the question of whether there is a moral reality or moral truth independent of our convictions" (Pogge, 2007, p. 163). Where meta-ethical beliefs do not speak directly to the theory being constructed, RE permits they may be sidelined; in other words, Rawls's method travels epistemically light. This allows for consensus to be built at the meso-level, leaving foundational questions up to individuals. Rather than a transcendent theory of moral truth, RE consequently constructs "something like a shareable standpoint from which individuals can see themselves and their surroundings" (Brandstedt & Brännmark, 2020, p. 364). Each of us can then reflect on the coherent whole, as presented, compare it to our own beliefs, and judge the reasons the theorist has given for their choices and commitments. If we find these to be justified, we can then decide whether or not to accept them for ourselves.

So far, however, we have only discussed the judgements and principles that a theorist will either have already held or else developed while carrying out their RE process. The resultant equilibrium would thus only be compelling to other individuals who also shared these considerations, and would hold little sway in a pluralistic society that included people with different starting points. Accordingly, such a 'narrow' RE at most provides a descriptive account of how a theorist's existing beliefs can be made coherent (Doorn, 2009, p. 128). But Rawls is clear that RE's demands for revision do not end here. Instead, as discussed, we must continue to reflect upon and assimilate new judgements as we become aware of them, whether from ongoing personal experience, seeking out new research, or discussing our views with others (Pogge, 2007, p. 165). Indeed, the justificatory power the method strives for can only come from pursuing this 'widening' process. This means my eventual RE could not simply have described my own initial, internal beliefs made coherent (Baderin, 2017, p. 4). Rawls (2001, p. 31) is clear that theorists must test their positions against various other moral and non-moral background theories, which could include anything from

other philosophies (e.g. utilitarian or Marxist approaches) to scientific findings[25]. And it is only by striving for coherence across all these levels of abstraction that a theorist's RE might eventually expand into a so-called 'wide' RE—one possessing the normative force to justify a position to others (Daniels, 1979, p. 259).

3.2.2 Public Reflective Equilibrium

So far, so good. The foregoing essentially describes RE orthodoxy. I will now, however, explain how my implementation of RE deviates from the Rawlsian status quo. This involves recognising that the RE procedure is generally a solitary endeavour, carried out by the theorist alone. Nonetheless, in the past twenty-five years or so, some innovative theorists—most notably David Miller (1999), Martine de Vries and Evert van Leeuwen (2009), Jonathan Wolff (2018, 2020), and Avner de-Shalit (2009)—have explored incorporating qualitative research into their theorising process. This modification is generally taken to increase the credibility and justificatory power of the resulting theory by, in effect, widening each theorist's RE (De Vries & Van Leeuwen, 2009, p. 494). In doing so, it helps expose the biases and misunderstandings we often uncover with ourselves when evaluating complex moral issues (Baderin, 2017, p. 14). Indeed, these theorists all report how having conversations with informed people throughout their research provided excellent opportunities to source views, test them, and incorporate new insights into their developing equilibria. This helped them establish an even closer fit between the empirical reality of a situation and their normative theorising—an outcome I am keen to replicate. I, too, consequently sought to incorporate inputs from others into my own equilibrating process.

Nevertheless, proposals for how to incorporate a 'public' into RE vary. While any part of the process could, in principle, involve other participants, three main approaches are common. The most prevalent involves identifying and favouring those judgements that are already "a matter of consensus within a group" (Strong, 2010, p. 135). These judgements, the suggestion goes, should possess some initial credibility due to the consensus they command. Yet this would seem to place popular judgements beyond reproach simply because of their popularity. It consequently resembles a form of foundationalism, and so would undermine RE's coherentism. Not only this, but privileging widely-held judgements would also seem to limit the potential for progress, adding a conservative twist to the process (Daniels, 1996, p. 40). Accordingly, this was not an approach I adopted. Rather than favouring judgements, however, one could alternatively source principles from public opinion. This would allow for "superficial" public attitudes to be "legitimately be set aside" (Baderin, 2017, p. 8). Miller prefers this solution, as he argues that drawing on widely-supported principles helps ensure that "the theory of justice appears no longer as an external

[25] Rawls, for instance, included "a theory of the person, a theory of procedural justice, general social theory, and a theory of the role of morality in society" (Daniels, 1979, p. 323).

imposition conjured up by the philosopher, but as *a clearer and more systematic statement of the principles that people already hold*" (Miller, 1999, p. 51). This suggestion suffers from similar issues, though. It likewise privileges existing principles, lending them unwarranted foundational status[26]. I consequently avoided this approach, too.

The final option is the most radical. Instead of publicly-sourcing judgements or principles, theorists can instead incorporate others into the equilibrating process itself. Motivation for this stems from the fact that, unlike with some methods, the theorist constructing an RE must take seriously the value pluralism that is central to liberalism. Rawls (2005, p. 50) tells us that solutions must be able to appeal, at least in theory, to a variety of 'reasonable' people; not individualistic or self-interested agents, solely pursuing their own ends, but rather citizens striving to co-create "a world in which they, as free and equal, can cooperate with others on terms all can accept". And what better way to arrive at a theory all can accept than by encouraging citizens to collaborate in its creation? There is definitely something intuitively and appealingly 'liberal' about this approach. Yet Alice Baderin (2017) has cast doubt on the practicality of a maximally-public procedure. As she argues, the feasibility of reaching a truly-communal RE, where all participants revise their beliefs to be in perfect harmony with one another, is not remotely clear. Not only are people unlikely to have begun theorising with identical sets of shared judgements, principles, and background theories, but they are also unlikely to have evaluated them in the identical ways required to reach a mutually-acceptable whole. The role of other people therefore needs to be more nuanced if RE is to be reached.

Thankfully, a workable model readily follows from moderating the role of the public. Here, Wolff and de-Shalit's *Disadvantage* (2007) and *City of Equals* (2024) provide invaluable templates. Although the two philosophers began their research with theoretical commitments and judgements of their own, they conducted qualitative interviews with people likely to possess specialist knowledge of the issues in question throughout[27]. By drawing on their participants' expertise and moral intuitions, but not privileging these inputs, Wolff and de-Shalit thus widened their understanding without taking popular inputs as static, conservative anchors. Instead, the interviews triggered regular opportunities for reflection. The philosophers constantly tested, revised, and enhanced their theory in light of interviewees' interventions (Wolff & de-Shalit, 2024, p. 18). As they write, "we did more than simply

[26] A further, practical problem is that, unlike philosophers, members of the public do not generally hold formalised, structured and non-conflicting understandings of moral and political principles (Baderin, 2017, pp. 11–12). It is therefore unclear how any principles—save for the most obvious, such as 'killing is wrong'—could by extracted for use in RE, except without significant interpretative work that could smuggle in bias on the part of the theorist.

[27] In one project, this was both disadvantaged individuals and those providing them with support (Wolff & de-Shalit, 2007, p. 12), in the other, this was city-dwellers from around the world (Wolff & de-Shalit, 2024, pp. 17–18).

learn about people's attitudes and views […] we revised and modified our theory according to the theories and intuitions expressed" (Wolff & de-Shalit, 2007, p. 12). This introduced novel insights to the RE process, adding deep theoretical and practical detail to their existing thinking (Wolff, 2020, p. 47). And, likely due to the feasibility issues with the maximally-public version of RE outlined above, Wolff is clear that the result was not a communal equilibrium—"although the method is public it remains entirely under the control of the theorist" (Wolff, 2020, p. 49). This is accordingly the 'co-constructive' flavour of RE I adopted.

3.3 Research Design

I have, so far, presented RE in quite abstract terms. But, over the remainder of this chapter, I will concretise my approach with notes about casing, my interviewees, the interviewing process, and how I went about integrating qualitative interviewing data into my RE. Firstly, the policy context surrounding contemporary British digital identity systems evidently forms my chosen case. This was partly a practical choice, but mostly driven by the country's theoretically-interesting situation. My principal aim, after all, is to construct a liberal, political-philosophical framework that will allow me to explore how the interrelated schemes that GDS and DSIT are developing could be integrated into a coherent RE. And the British context is particularly well-suited to this task, as we will see. Not only has Britain always been, "at the forefront of the development of identification technologies" but, as Higgs (2011, p. 9) provocatively asked over a decade ago, why should "a country that prided itself historically on leaving people alone […] now be a world leader in their surveillance and tracking"? Given Britain's decades of experimentation with different digital identity architectures, it thus provides the ideal case study for exploring the normative issues surrounding different approaches to identification. In particular, being able to chart the movement from centralised identity cards to a federated ecosystem, and the later combination of these two approaches, will provide ripe opportunity for internal comparison and deep analysis of the two prevailing models.

Practically-speaking, this focus also allowed me make good use of the experts with whom I already had existing professional relationships. As I knew I wanted to involve other participants in my RE from the outset, the bar for doing this was accordingly lower in Britain than elsewhere. At the same time, while normative research into British digital identity systems more generally has always been relatively scant, I realised early on during my review of the literature that this kind of research had almost completely dried over the past decade. Even though valuable work in a similar vein was proliferating around the study of international systems—particularly, as we saw, in Europe and across much of the global South—it simply was not at home. There was thus an obvious gap to fill. Britain was, after all, going through a particularly interesting transition during my first few years of research, and is again now. And although Verify's federated model eventually failed domestically, the approach has since been emulated internationally, with groups in America (NIST),

Canada (Pan-Canadian Trust Framework), Africa[28] (SATA) and Europe (eIDAS)—not to mention Scotland (ScotGov)—all now pursuing similar models. The project's theoretical import would therefore not be limited to Britain alone, though I knew the scope of any generalisations would need, as I explain later, to nevertheless remain limited.

With my case selected, the earliest stages of my research design were then motivated by further consideration of various background theories, and their link to my overall epistemic project. As two pioneers in the RE space, Christoph Baumberger and Georg Brun (2021, p. 7927), explain:

> [In RE] the background is treated as independently justified to some degree, but not as being immune from revision on principle. Consequently, the contrast between foreground and background is established by the epistemic project at hand and reflects the fact that inquiry cannot but proceed piecemeal, even though justification is ultimately holistic; that is, a matter of a reflective equilibrium that encompasses all the epistemic agent's commitments.

Specifying the nature of epistemic project I am pursuing was thus highly important. Primarily, it defined which normative and empirical features of the British identity landscape would function as the agreed-upon background, against which the bulk of my work in this thesis would take place. By now, it should accordingly be clear that the Literature Review sketches a large part of this 'independently justified' backdrop. It summarises many of the relevant background theories (especially the fundamentals of liberalism and digital identities, as well as sociological accounts of modern digital identity systems) that will underpin the more detailed discussions of liberal theory and its intersections with identification systems yet to come.

At the same time, defining my epistemic project also helped firm-up my conceptual framework. As Dietmar Hübner argues (2017, p. 13), this is vital in RE for "connecting different levels of normative reasoning in a clear-cut manner and thus allowing for their hermeneutical deepening and reciprocal balancing". In my case, then, a liberalism attuned to the British context provides this framework. It grounded my RE within a "definite setting", and so ensured the process was carried out in a principled rather than "arbitrary" manner (Hübner, 2017, p. 15). After all, unrelated elements from different conceptual frameworks cannot be bundled together haphazardly. For the RE process to result in a holistic, cogent, and rational whole, a tightening or 'pulling together' of all the strands involved is required—this is what Hübner means by hermeneutical deepening. And, in the British case, liberal common law provides this context. I therefore did not fully consider every alternative normative theory that could possibly have grounded this work. I did not, for instance,

[28] I should disclose that, from December 2020 until March 2021, I worked with the Digital Equity Association to develop a federated, cross-continental identity scheme to underpin a digital economy in the region.

construct multiple equilibria from Confucian, Marxist, and Republican perspectives, then compare and contrast them all. Rather, consideration of competing views was carried out only so far as it was necessary to cast my characteristically-British approach into sharper relief. It was, after all, generating a coherent *liberal* framework that was my ultimate goal—and this had to be constantly borne in mind.

Finally, bounding my epistemic project also precluded the need for extensive speculation about how previous British governments could have acted. Such counterfactuals were just not relevant for current systems, except where lessons could be drawn. Instead, I was developing an account of where "to go, starting from here, which is of course what the government needs to know" with regards to policy (Wolff & de-Shalit, 2007, p. 11). As Wolff (2011, pp. 6–7) elsewhere reminds us, this requires the theorist "to understand why it is we have the policies we do have before advocating change." Consequently, it was only by first building my understanding of historical British identity policy that I could construct the theoretical footings needed for detailed discussion of the issues facing Starmer's government today. That said, remember that no single element of RE is ever beyond reproach. As the process advanced, aspects of the background did indeed end-up needing to be revised. Nonetheless, in previous chapters I hope to have sufficiently detailed both my initial position and preliminary understanding of the theoretical landscape for readers to decide whether or not we started from shared beginnings[29]. And, although our assumptions might well differ, at least allowing readers to identify these points of divergence before the equilibrating begins in earnest should be made easier by my attempts to be transparent about these starting points.

3.3.1 Which Public?

With the scope of my project set, one of the first tasks was then, of course, deciding who to interview—i.e. from which 'public' to draw. Much like Wolff and de-Shalit, I wanted to include a range of participants that each possessed unique perspectives on my chosen case. Identity policy is, however, a highly-technical and relatively misunderstood topic. Early on, I therefore decided not to interview members of the general public, and to instead draw primarily on the views of elites and experts. While 'normal' people may well have provided valuable insights, I simply found that there were other ways to effectively source the kinds of inputs they might have made. The press, for instance, regularly reports on noteworthy identity cases involving citizens, and many experts I spoke to had already aggregated large amounts of user research to inform their thinking. Both DSIT and GDS also commissioned Calls for Evidence during the project, with the former even publishing a 'public dialogue'

[29] This echoes a call from Mark Coeckelbergh (2018, p. 5) for theorists to make explicit their "often salient, (descriptive) social-ontological and (normative) political-ideological assumptions." Although he does not explicitly employ RE, Coeckelbergh implores fellow philosophers of technology to pay closer attention to political philosophical methods.

report while I was writing up, which drew on weeks of workshops with members of the public (DSIT, 2024b). I consequently found that these sources surfaced sufficient content to inform my understanding of digital identity systems from the user's perspective. As a result, only a few of those interviewed, and even then only incidentally, were everyday users of the systems we discussed.

However, with DSIT and GDS's schemes both still in 'beta' during my primary fieldwork period, I soon realised I could not exclusively interview experts working on these projects. Not only were the programmes undergoing active testing and development, which limited my access, but both were also fundamentally reactions to the wider historical and political context around identity policy. I therefore decided to seek out a wider cross-section of participants that could illuminate different aspects of Britain's long-running struggles with identity—especially those who could unpack the parallels with prior systems. This included senior professionals that had worked across the public and private sectors over the past twenty-five years, as well third-sector actors that might harbour outside perspectives (c.f. Bryman, 2012, p. 418). But this meant the scale of my conclusions had to be limited. As I would only be considering the views of a relatively narrow range of individuals, I could not generalise much beyond the British institutional context. My interviews are therefore best understood as "a springboard from which to philosophize and theorize", which were nonetheless valuable "provided that we keep in mind that statistically this data should be taken with a pinch of salt" (Wolff & de-Shalit, 2007, p. 190). The goal, after all, was to ensure that my political theorising remained tied to empirical reality via expert engagement. It was not to generate statistically-defensible claims about the British public's opinions[30].

3.3.2 Ethical Considerations

With my 'public' selected, the next step was to secure ethical approval and actually conduct the interviews. This part of the project went through a rigorous review process, led by the Central University Research Ethics Committee[31] (CUREC). Overall, though, this was a relatively straightforward hurdle. The risks to participants were relatively minor, given I was not going to be interviewing vulnerable groups, with only one potential conflict of interest on my own part the main concern—at least at the project's outset. This issue arose because many interviewees had interacted with the Open Identity Exchange (OIX), a former trade association for UK digital identity

[30] As Wolff and de-Shalit (2007, p. 190) make clear, carrying out enough interviews to cover a statistically-relevant sample of the general population would be immensely costly—far too costly for a doctoral project. This would have been a much different project; closer to something a sociologist or politics researcher might have led, but not one that a political philosopher like myself would be best-placed to carry out.

[31] Oxford University Social Sciences and Humanities Interdivisional Research Ethics Committee Approval Reference: SSH_OII_CIA_21_005.

providers that I was employed with on a part-time basis for most of my DPhil. As a result, the CUREC process helped me recognise that a) information gleaned from interviews could be of potential commercial value to the OIX, and b) interviewees may have tried to get me to share business-sensitive OIX information with them. To mitigate these risks, I therefore made sure my association with OIX was raised at multiple points before and during the interviews. I also reiterated that any sensitive information would be treated with the utmost confidence, and reassured interviewees that I would not pass any information either way. Ahead of the interviews, I also outlined the data protection laws (mainly the UK's General Data Protection Regulation, or GDPR) that would govern the collection and processing of any data arising from our interactions.

Despite this potential issue, I believe the OIX connection ultimately ended up being a net-positive, not least because the chief strategist is well-liked and respected within the community. In actual fact, OIX hired me precisely because they were happy to help introduce me to contacts, and thought it would be a mutually beneficial partnership. This was a key reason I took the job. My association with the chief strategist and the OIX brand thus opened doors to several participants I would not otherwise have been able to interview. Indeed, through these connections, I was eventually invited to apply for a digital identity policy job at DSIT in 2023, towards the conclusion of my project. This presented a further conflict of interest—though, as I was into the writing-up stage by this point, the scope for conflict was still limited. I had already completed all my interviews, so most of my understanding of DSIT's scheme predated my time at the department. This made the potential ethical challenges easier to navigate. I agreed with the hiring manager that I would retain academic freedom, so long as I used no privileged information gleaned through my time at DSIT in my thesis. I can confirm I have respected this condition. Though the role has no doubt sharpened my understanding of digital identity, any views expressed in the final substantial chapter, which critiques DSIT's current policies, were constructed from information available to me before I began working at the department.

Returning to the ethical considerations surrounding the interviews, the other notable risk related to attribution. To tackle this, I obtained explicit consent via email in advance of any interviews, mainly so that the scope of the relationship could be pre-agreed. I then reiterated the implications of this written agreement at the start of each interview to ensure understanding. A few participants failed to agree in advance but, as I was recording their interviews, I made sure to capture a record of oral consent as an alternative. In all cases, I also made clear whether we would be talking 'on' or 'off the record' and ensured that participants understood the extent to which they would be able to correct factual errors after the interview. I also offered the option of pseudonymity as a mitigation strategy. However, the overwhelming majority of participants agreed to take part mostly 'on the record', orally flagging only certain moments of discussion as 'background'. This surprised me. I had expected far more

to take up the offer of pseudonymity. And, in the end, seven of the eight interviewees who took part on condition of pseudonymity understandably only did so because governmental policy limited their public statements. With hindsight, the desire to be credited in print should perhaps have been expected—after all, many of the participants I spoke to trade on their reputations as thought leaders. But I nevertheless was pleased that so many interviewees could participate openly.

Finally, protecting the data I gathered throughout the process was also vital. Even if interviewees were generally happy to speak on the record, specific sections of many conversations were not to be quoted. I therefore stored all recordings, which were made digitally, on an encrypted drive, on a firewalled device, and only backed these up locally to another encrypted drive. Transcription and analysis was also carried out manually, on the same local device, rather than relying on cloud-based tools. Additionally, codenames were used to refer to pseudonymous participants, which meant that I possessed a digital master list for identifying pseudonymous participants throughout the project. This was kept secure in the same secure manner as my other data. The final element of ensuring my data's integrity—and so its value for my theorising—involved checking any quotes that made it into my RE against the record, running named quotes past the participants involved. This helped to guarantee my work's accuracy and ensured that I was not putting participants at any risk by quoting specific passages of our discussions which they were not expecting. It also provided a good opportunity to stay in contact. By the project's conclusion, any remaining data will then promptly be deleted. This should mitigate any residual data-related risks, and mark the end-point of my research.

3.4 Interviewing and Equilibration

I will now describe the interviewing process itself, as well as how this interacted with my RE. I began recruitment soon after achieving ethical approval. As noted, several individuals were already known to me—via OIX or due to their status as members of the 'identerati', the tongue-in-cheek phrase that some actors in the industry use to refer to themselves. I therefore approached recruitment and sampling via the snowballing method. This seemed the best way to gain access to senior participants, relying on the power of social vouches. Indeed, it is generally considered the only feasible approach for sampling these sorts of populations (Bryman, 2012, p. 203). Through referrals sourced from a series of initial interviews with pre-existing connections, I built a network of interviewees that together provided a holistic overview of the digital identity space. As time went on, I also reached out to some participants 'cold', mostly via email or social media, when suitable referrals could not be secured. Although the resulting sample cannot consequently be called statistically relevant, I have already discussed why this is not a problem for RE purposes. I should also note that participants were not paid but, in lieu of payment, many did request to be kept informed about the project as a condition of their involvement. I was happy

to accept these terms, not least because it meant the door would remain open for additional engagement later on in the project.

All-told, I interviewed fifty-one experts from all sides of the identity debate. The final group encompassed everyone from senior civil servants, government contractors, consultants, and senior employees at identity companies, to civil society actors, critics, and one journalist. Many had occupied multiple roles across these sectors over their careers, sometimes simultaneously. Unsurprisingly, most also lived in the UK or had worked on British identity projects over the years. Of those who had not, their insights were general and important enough that they had still either influenced British policy and the market, or else held transferable opinions that were of interest. A tabulated breakdown of the interviewees can be found below:

Name[32]	**Job Title**	**Organisation**
Adam Cooper	Director	ID Crowd
Alastair Johnson	Founder	Nuggets
Alexander Blandford	Independent Contractor	Various Organisations/Ex-DCMS
Alison McDowell	Government Contractor	Beruku
Andre Durand	Founder and CEO	Ping Identity
Andrew Bud	Founder and CEO	iProov
Andrew Hindle	Independent Contractor	Various
Benjamin Welby	Policy Professional	OECD/Ex-Government Digital Service
Bryan Glick	Journalist	Computer Weekly
Colin Wallis	Executive Director	Kantara Initiative
Daniel Goldschieder	Founder and Executive Director	Open Wallet Foundation
Dave Allen	Head of Business Development	Charteris
David Birch	Consultant	Consult Hyperion
David Black	Consultant	ID Crowd
David Rennie	Director of Digital Identity Market Strategy	IDEMIA
Dick Dekkers	Director of Business Development	Digidentity
Don Thibeau	Executive Director	The OpenID Foundation
Drummond Reed	Chief Trust Officer	Evernym
Elinor Hull	Identity Services Director	Post Office
Emma Lindley	Co-Founder and Chair	Women in Identity
Eve Maler	CTO	ForgeRock
Gilad Rosner	Independent Consultant	Various Organisations
Guy Herbert	Privacy Campaigner	NO2ID
Heather Hinton	CISO	RingCentral
Ian Glazer	Founder and President	Weave Identity
Jeremy Grant	Managing Director	NIST/US Government

[32] Please note: Some participants chose to obfuscate their details for privacy reasons.

Name[32]	**Job Title**	**Organisation**
John Erik Setsaas	Vice President of Identity and Innovation	Signicat
John Haggard	Chief Business Officer	Yubico
Jon Nash	Fellow	Demos
Joni Brennan	President	DIACC
Joseph Spear	Director of Communications	Mvine Ltd.
Kaliya Young	Independent Consultant	Identity Woman/IIW
Louise Maynard-Atem	Head of Data Insights	GBG/Women in Identity
Martyn Taylor	Senior Civil Servant	Government Digital Service
Melis Mevsimler	Fellow	Ada Lovelace Institute
Mike Bracken	Founding Partner	Public Digital/Ex-GDS
Nick Mothershaw	Chief Identity Strategist	Open Identity Exchange
Pieter Kasselmam	Principal Program Manager	Microsoft
Phil Windley	Senior Software Development Manager	Amazon Web Services Identity/IIW
Steve Pannifer	CEO	Consult Hyperion
Stephen Wilson	Founder	Lockstep Consulting
Tom Fisher	Research Officer	Privacy International
Tony Fish	Independent Consultant	Various Organisations
*	Policy Professional	Yoti
*	Privacy Campaigner	Various Civil Society Groups
*	Senior Civil Servant	Department for Digital, Culture, Media and Sport
*	Policy Professional	Department for Digital, Culture, Media and Sport
*	Policy Professional	Department for Digital, Culture, Media and Sport
*	Senior Civil Servant	Department for Work and Pensions
*	Senior Civil Servant	Government Digital Service
*	Policy Professional	Tony Blair Institute for Global Change

Table 1 — List of interview participants

3.4.1 Data Collection

After a handful of pilot interviews in early-2021, the bulk of my data collection took place between September 2021 and June 2022. Almost all interviews were conducted synchronously over videocalling software, with the exception of a few carried out in-person at an industry conference in the Summer of 2023. While, with hindsight, I would have preferred to have conducted a couple of the higher-stakes interviews in person[33], the ongoing effects of the coronavirus pandemic made this all-

[33] Only one participant did not take the digital interviewing process seriously, and I think this issue would have been mitigated if the interview had been in-person. They took the call whilst walking to

but impossible[34]. Thankfully, research suggests there are, in general, no "limitations inherent" to interviewing digitally rather than in-person (Hanna & Mwale, 2017, p. 261). And my general impression was that digital interviewing is a highly rewarding and effective way to widen an RE. Proceeding digitally also made recruitment easier, not least by ensuring that travel was not required (Hanna & Mwale, 2017, p. 262). Several participants even remarked that they could only 'fit me in' because of the flexibility that digital interviewing offered. When it came to ending recruitment, I continued until it appeared I had reached saturation of both individuals and views. As participants starting reaching too far afield for snowballing recommendations, and especially when no new perspectives or ideas were coming up, I wrapped up the primary interviewing stage of the project. This is considered best practice in both qualitative research design and empirical political theory (Zapata-Barrero, 2018, p. 81).

Each interview lasted between ninety minutes and two hours. They were semi-structured to allow for the exploration of broad themes without expecting to arrive at definitive conclusions (Bryman, 2012, p. 403). This helped me gain an overview of my interviewees' thoughts without imposing a rigid framework upon the interview format—allowing me to recognise and respect their expertise (Bryman, 2012, p. 471). Another benefit of this approach was that I could tailor questions to the participant, with CEOs not asked about the intricacies of setting governmental policy, for instance. That said, this was mostly a fine tuning exercise. Approximately three quarters of each interview covered the same basic material. Given that the interviews were conducted over a year or so, however, my questions did evolve as my own thinking was refined. To begin with, I certainly knew little about digital identity systems—and likely asked some naive questions. This was despite the fact that I had, following Wolff and de-Shalit (2024, p. 55), not approached the interviews "with a blank piece of paper". I had already read and reflected on a lot of material before beginning my data collection. But the whole point of the interviews was to test and challenge my position; to "modify, enrich, and ultimately specify" my theoretical understanding (Wolff & de-Shalit, 2024, p. 55). By the end of the project, I consequently like to think I knew a little more than I did at the outset, and that this translated into more thoughtful questioning.

---

the supermarket, clearly distracted, then kept me on hold for fifteen minutes while they shopped. I ended the call soon after they returned. Thankfully, this was the only disappointment, with every single other interviewee engaging fully with the process.

[34] As coronavirus restrictions lifted I did begin to meet participants I had previously interviewed at various industry events in 2021 and 2022. This included the biggest US and UK conferences, like 'Identiverse', 'Identity Week Europe', and the OIX 'Identity Trust Conference', as well as the Alan Turing Institute's 'Trustworthy Digital Identity Conference' and other smaller events. These provided welcome situations for informal follow-ups with interviewees. They also occasionally helped with recruitment. I only got to interview certain senior civil servants and members of the press, for instance, after meeting them face-to-face at these conferences. These participants were generally harder to contact via the industry channels I initially had available to me.

The first half of each interview generally involved some discussion of the participant's background, as a warm-up, followed by questions designed to gauge their opinions about both historical and contemporary (digital) identity policy in Britain. The purpose was to source judgements about the government's plans, past and present, as well as about the wider identity industry. Generally, I found participants had a good grasp of recent identity developments. There was also a surprising amount of agreement when it came to diagnosing the issues with previous governmental systems; a consensus of sorts had definitely emerged around identity cards and Verify, as well as how best to address each scheme's shortcomings. I therefore attempted to challenge this view wherever possible, not least to ensure my own understanding. Overall, I also tried to surface both factual data about how systems worked and value data about why participants thought they were designed to work in that way. This was vital for ensuring my reflections could eventually lead to policy suggestions. As Wolff (2011, p. 5) notes, in most contexts "some public policy will be in place, and in most circumstances the burden of argument for change is higher than for reflective or unreflective continuation of current policy". Understanding the status quo was thus an essential precursor to suggesting any movement beyond it. But this part of the interview also allowed me to grasp a participant's level of understanding—were they a technical expert, or could they speak more to social and even conceptual issues?

The second half then turned towards these conceptual issues and attempted to elicit general normative insights. Initially, I was not sure whether participants would be able to contribute at this level. After all, the discussion veered towards quite abstract considerations of rights, goods, and the nature of citizenship, as well as the changing relationship between citizens and the state. But I need not have worried—most participants were highly-qualified, educated professionals working in an exceptionally normatively-charged space. For them to not have come across these kinds of issues, which often feature (at least implicitly) in the debates around national identity systems, would have been surprising. In actuality, theoretical engagement was thus high, particularly amongst the consultants and more senior participants. Normatively-couched language often required some coaxing on my part, and this was where a more co-creative approach definitely showed its worth but, where participants could engage, their contributions were often pleasingly nuanced. I consequently gained significantly more material to integrate into my theorising at this stage than I originally expected. Finally, after a few lighter questions intended to help prime my snowballing requests, I concluded each interview. I would then send a brief follow-up note of thanks, and turn to transcribing and analysing the interviews—the former immediately after each discussion, the latter in batches, later on.

3.4.2 Analysis and Reconstruction

What did interview analysis involve? Qualitative data fed constantly into the ongoing mutual adjustment process that I was carrying out. To explain, it is important

to detail how exactly my RE interacted with the empirical research over the entire course of this project. There were three overall stages. The first involved constructing an initial, narrow RE that brought together my own considered judgements and principles. This work preceded the interviews, and was undertaken alone while I wrote the first draft of my Literature Review and reflected on my initial position. As this process followed the standard RE steps outlined towards the beginning of this chapter, I will not recap what was involved. More unusually, I then carried out the second stage concurrently with the interviews. This is where I began to widen my narrow RE with input from my participants, and worked to ensure a tighter fit between my understanding and the reality of the situation as understood by on-the-ground experts. Looking back, this was undoubtedly the most theoretically-productive and enjoyable part of the process. Most of the advances in my thinking occurred at this co-constructive stage, in collaboration with my participants. Lastly, a reconstruction stage rounded out the process, which I will expand upon shortly. It was here that I properly coded my data, finalised my RE, and began to write my position up into the chapters that constitute the remainder of this thesis.

Before expanding on the final stage, let me detail the initial interview analysis that went into the second. While I was carrying out my primary data collection, I opted to keep any analysis light and fluid. I therefore did not employ any formal coding techniques at this stage—this part of the process was purposefully kept more intuitive. In the co-constructive stage, I was after all mostly looking to test and refine the considered judgements and principles I had already brought into a narrow RE with my participants, as well as source from them new judgements and principles (and, to a lesser extent, background theories) that might help challenge or strengthen my existing views. I accordingly focused primarily on soliciting judgements—gathering a range of stakeholder opinions to inform my theory-building, as this was where on-the-ground knowledge really shone through and highlighted the many lacunae in my initial view. That said, I did engage interviewees who showed sufficient theoretical interest at the level of principles and/or background theories. Many interviewees thus contributed at all levels of abstraction, though I should stress that some primarily engaged at the level of judgement. This did not, however, preclude me later trying to derive principles from their judgements during my own equilibrations.

My goal at this stage was not "to evaluate the 'truth' of a position, but rather to analyse the fact that there is a real conflict of positions" (Zapata-Barrero, 2018, p. 81). In other words, my aim was to bring out various actors' concrete interpretations of the normative problem space. This was why I kept any initial analysis very light. Although I needed to approach the interviews with a preliminary set of considered judgements and principles of my own, so that we might have some mutual groundwork to build from, I would also not reveal my own views straight away. I began instead by asking participants to explain the problem space in their own words, before reframing and seeing where any agreement or disagreement arose. Being relatively upfront with my initial commitments made them "available for rational

debate" and contestation (Susskind, 2020, p. 86), and ensured I 'showed my premises' in line with De Vries and Van Leeuwen's (2009, p. 495) rules for RE best practice. But, by only revealing many of my judgements and principles once participants had already outlined theirs, I nevertheless tried to ensure I would not bias their own framings. I suspect this was relatively successful in practice, not least because the people I was interviewing often had far more developed and strongly-held views than I did. Indeed, I was usually the one learning new framings, not my participants.

During the interviewing period, I was constantly revising my judgements to make them better cohere with my ever-developing set of principles. The process continued well into the beginning of my write-up, until something like a stable equilibrium began to emerge. I repeatedly went back and forth between theory and practice (c.f. De Vries & Van Leeuwen, 2009, p. 492), motivated by the belief that "[e]mpirical and ethical theory ought both to be used, and used in tandem, to guide public policymaking" (Goodin, 1992, p. 4). Theory in this case meant academic research, especially relating to the historical content I was beginning to write alongside the interviews, as well as any theoretical discussions I had with my interviewees. Interviewing, on the other hand, provided almost all of the practice-relevant insights[35]. Over the course of this cyclical process, I also came to notice that many participants shared similar talking points. I recognised these from other interviews, desk research, and my own understanding. As my familiarity with the debates grew, these repeated talking points thus helped alert me to when I was nearing saturation around various topics. I would then move onto a new area of discussion. As the interviews progressed, a theoretical scaffold that retained a close relationship to a range of real-world policy concerns thus took shape. This was stage two: the co-constructed, widened public equilibrium.

Completing this stage helped me gain a holistic understanding of the current policy context. It brought the relevant values and assumptions underpinning digital identity into sharper focus. And it was for precisely this reason that I had aimed to gather situated knowledge from a range of differently-located participants in the first place (J Reinecke *et al.*, 2016, p. xiv), taking seriously interviewees' differing perspectives to reflect an interpretive approach to interviewing (Edwards & Holland, 2013, p. 16). It was accordingly rewarding to see RE theory unfold in practice. Of course, I did not find an overall position that all interviewees agreed upon. But this was to be expected after having read Baderin's work. My participants and I disagreed about many points, and often were coming at the problems from ideologically diverse starting points. But the process did robustly test my views and do much to firm-up my position—which shifted quite drastically from where I began, as will become clear in later chapters. For these reasons, I am confident the interviews helped ensure that

[35] My employment at the OIX rarely exposed me to much identity practice. At most, I had some limited exposure at the industry trade shows and conferences mentioned above.

my theorising was exposed "to the full force of critique from explanatory theory and empirically grounded research" required to try and generate a wider RE (Bauböck, 2008, p. 60). And, although widening is of course a process that is never really finished, I can nevertheless claim to have given it a good go.

However, I eventually realised I could not end the process here. This is when the need for a final reconstruction stage became apparent; a concept I adapted from Baumberger and Brun (2021). Although Baumberger and Brun submit that the details of each person's equilibrating process will always be project-dependent, they emphasise that, whatever the project, reconstructing an RE not only contributes to its justification, but is also the only way for the theorist to divine the "precise configuration" of moves and values that drove their theorising throughout (Baumberger & Brun, 2021, p. 7937). In other words, it is only once a candidate RE has been constructed that the theorist can retrospectively discern the most important drivers of their equilibration, which they can then use to reconstruct it for justificatory purposes. In my case, because my RE had developed over the months of interviews, and continued to develop as I began writing-up, I realised that it would also be necessary to go back and review all of my data in light of my updated understanding of the policy area as part of this reconstruction process. Essentially, I had to conduct another round of interview analysis, going back over all of my transcripts to see if I had missed any insights the first time around. After all, during the earlier interviews I had still been building my understanding of the problem space, which left plenty of room for misinterpretation on my side.

Properly coding the interviews and extracting themes, not to mention grouping these themes and looking for connections, added a significant amount of additional depth to my understanding of the policy area and my developing RE. That said, I did not code entire interview recordings. By this stage, I knew that much of the content was simply not relevant. This is not to say it was not useful to the interview process at the time. It was certainly necessary to 'warm up' participants and build rapport, particularly as I had not met most of these people before. But only snippets of each discussion now bore direct relevance to my RE at this final stage of the process. I therefore screened the interview transcripts I had made previously, only formally coding a) sections containing novel insights that required further reflection, or b) any key ideas or themes that I retrospectively identified as having influenced my thinking. Though I would characterise the initial, informal analysis I carried out as deductive, this 'focused' or 'selective' approach to coding during the reconstruction stage was consequently inductive. I did, after all, come back to the interviews with an RE that allowed me to identify relative passages for closer analysis. Theory therefore took some precedence at this closing stage of the process, and these codes and themes then fed into the final reconstruction of my RE.

3.5 Conclusion

By way of a conclusion to this chapter and, indeed, *Part I*, let me summarise how the rest of my reconstructed RE unfolds. Over the following chapters, I weave together qualitative interview data, my own observations and views, as well as insights from the literature. This reconstruction is intended to help a reader understand how I arrived at my position. Again following Wolff and de-Shalit (2024, p. 56), I do not therefore include full transcripts of all my interviews, and instead draw on only those "most illuminating" extracts and themes that added the most to my developing equilibrium. I should also note that what follows is presented chronologically, although this does not reflect how my thinking actually developed. The argument spans several hundred years of British history, albeit with a bias towards the past twenty-five years or so. This is because the digital systems that emerged during this period are the most important for understanding contemporary systems and policies, though historical systems will, of course, provide useful context. But the remainder of this thesis is not a record of how my position evolved in real-time, as the circular iterativity of the RE process is impossible to capture in narrative form (CH Smith, 2023). Instead, what follows is intended to be made sense of from an external point of view. It accordingly presents the arguments that constitute my position in a way which is hopefully intelligible to others.

Before we get to that, though, in this chapter I have defended the specific form of politically-engaged theorising I elected to use for this project—a co-constructive version of public reflective equilibrium. And I have further justified both my focus on the British case as well as my decision to integrate expert views into my RE. Altogether, I have shown how this coherentist approach will empower me to weave an empirically-sensitive theoretical scaffold around my chosen case study over the remainder of this thesis. However, let me be clear. There will always be alternative ways of interpreting the inputs and carrying out the process of equilibration. You may well accordingly disagree with how I chose to balance various elements, or think I have overlooked key judgements or principles. Yet this is the price of this method, and operating in the messy reality of politics—even I will no doubt come to diverge from this position in the future. Nevertheless, I am confident that I have captured the British identity landscape sufficiently accurately to have arrived at an informed view that most would agree is fair, and can say that I have reached a stable equilibrium, at least for now. My task now, then, is to convey this position to you and, by doing so, address my overarching research questions. And this begins with an exploration of the history of identification systems in Britain, covering the period before the digital revolution.

—Part II—

Chapter 4.

Before Digital Identity Systems in Britain

> "If the political is to exist, one must know who everyone is, who is a friend and who is an enemy, and this knowing is not in the mode of theoretical knowledge, but in one of practical identification: knowing consists here in knowing how to identify the friend and the enemy."
>
> *– Carl Schmitt, quoted in (Derrida, 1997)*

To properly understand Britain's digital identity systems, we must first appraise the island's history. What transpires from evaluating the technologies and practices that modern systems have evolved from is that 'identification' in the technical, formal, and legal sense in which we generally use it today is an exceptionally recent phenomenon. Rationalising the population through such techniques came late to Britain. Developing identity systems oriented around the enumeration and management of individuals, whether analogue or digital, was simply not much of a priority for the central information state, which has traditionally relied on far less specific technologies for making populations legible. For most of British history, identity was instead left, by and large, to individuals to navigate amongst themselves; a social and performative exercise, at least for those of good standing. Yet when change finally did arrive, the effects were dramatic. New systems of paper-based management radically altered the relationship between the people and the state. Tracing the development of these novel technologies throughout the Industrial Age [36] —from signatures, seals, and registers up until the earliest days of computerisation—this chapter accordingly shows how the British state centralised a number of identification practices over this period, primarily through its displacement of the local and performative means of identification that had previously sufficed.

In particular, as technological development accelerated in the wake of two World Wars, the changes for normal people stacked up. As citizenship replaced subjecthood in the twentieth century, and became tied to political rights via new technologies and the emerging welfare state, formal identification was made to matter to ordinary

[36] The Industrial Age spanned the roughly two hundred years between 1760 and 1970.

people. In the main, these changes impacted the freedom, or liberty, of individuals living in Britain. Traditional, laissez-faire respect for negative liberty, as championed by so-called classical liberals, came under increasing pressure from social reformers that cared about the material conditions in which people languished. Accompanying the latter's far more positive notion of liberty, with its genesis in Victorian desires to address various social ills, increasingly centralised systems therefore newly-enabled the state to interfere more directly in the lives of citizens. Yet before this point, as we will see, centralised identification systems had surprisingly exerted next to no effect on the day-to-day liberties of British subjects, or even aliens. Illuminating the recency of this development will therefore clarify how dramatic any further normalisation of centralised identification practices in our modern digital era would be; a significant break with past customs. This context will then help me to explain, in chapters to come, why the state's recent forays into developing digital identity systems have faced so many setbacks.

3.1 Historical Identification Practices

From a contemporary vantage point, it can be difficult to imagine a time before widespread formal identification in Britain. Today, almost every important transaction or interaction we make involves some proof of identity that can eventually be traced back to the state—and official identities are seen as essential for ensuring the continued administrative functioning of modern governments (Caplan & Torpey, 2001). As historian Edward Higgs (2011, p. 2) summarises, people today "are registered and recorded from birth to death, and at various points in-between." Anything from driving a car, getting a job, paying tax, receiving benefits, or claiming a state pension depends upon submitting to a range of state identification apparatuses. Similarly, many non-governmental activities, such as taking out a mortgage or insurance, holidaying abroad, opening a bank account or requesting a credit check, all rely upon a series of carefully-choreographed collaborations between the state and commercial entities. These help ensure trust in who we are, as well as our entitlements to various products and services. We are constantly presenting organisations with proofs that attest to our age or eligibility (such as, that we are over-eighteen or have the Right to Rent), aspects of our identity (that I am Charlie Smith, or this is my customer number), or even, in recent memory, that we have been sufficiently vaccinated to safely take part in society. Identification is becoming ubiquitous in modern Britain.

Yet this state of affairs is rather exceptional. For the vast majority of British history, any notion of recourse to official identification systems to prove these kinds of claims would have been completely foreign to the average person (AJP Taylor, 1965, p. 1). As Higgs (2011) notes, formal identification methods were almost entirely reserved for criminals, aliens, and the dead, well into the twentieth century—and, even then, such records were overwhelmingly managed locally, relying on community knowledge rather than standardised and centralised bureaucratic systems. There were simply no

central records to consult; no one in Whitehall would have collected or maintained them. Policing was, for instance, led by parish constables who, much like district coroners, relied on the community to help recognise criminals and identify corpses. Even identifying beneficiaries of the Poor Laws—under the earliest vestiges of the welfare state—was handled locally, by each parish's Overseer of the Poor (Higgs, 2011, p. 47). In fact, likely the closest thing to a formal, nation-scale identification system in pre-modern Britain would have been the crude descriptions of rogues and frauds that merchants and magistrates circulated via the Hue and Cry and other private newspapers (Higgs, 2011, p. 106). The state, inasmuch as a unified state existed in Britain before the twentieth century, simply lacked the motivation and means for identifying most of its subjects given its highly-decentralised nature (Hall, 1985).

Law-abiding subjects, and especially the most well-to-do members of society, would therefore have been appalled at requests to identify themselves in the eyes of 'the state' (AJP Taylor, 1965, p. 1). Such demands would have been an affront to their honour. Rather than presenting formal identification papers, like many of their European neighbours, the average person would instead have primarily asserted who they were through social performances to their peers, along the lines outlined by sociologist Erving Goffman (1959). Tokens of identity like signatures and seals certainly played (largely performative) roles in business and legal dealings, but the state held no central records against which these could be checked or validated (Higgs, 2011, p. 59). Who you knew, what clothes you wore, and how you spoke were far more important markers of identity than any state-backed documentation you might present. Even the most formal transactions, such as matters of property and credit, were entirely handled via personal identification methods, such as vouching, testifying, and other community sources of knowledge (Higgs, 2011, p. 44). For much of British history, then, the idea of relying on the central state for an identity, let alone proving it with government-issued papers or cards, would have been risible. Recourse to state-run systems was simply not necessary. Identity resided in an individual's localities and networks, meaning identification was a irreducibly social, not technical, activity.

3.1.1 A Sociological Anomaly

The peculiarity of this situation warrants particular attention, not least because the general British reticence to build-out any state identification infrastructure—at least on home turf—stands at odds with the received sociological narrative around the changing nature of identification in the Industrial Age. In Daniel Bell's (1973) classically Weberian formulation, for instance, progressive rationalisation in the eighteenth and nineteenth centuries generated efficiency and productivity gains throughout society, driving the population away from a distributed, agrarian way of life and towards an increasingly centralised, urbanised existence (c.f. Webster, 2014, pp. 45–47). This capitalist development is thus taken to have engendered such anonymity in Britain's newly burgeoning cities and towns that the face-to-face, social

methods of identification that previously sufficed were rendered ineffective (Higgs, 2009, p. 349). In the emerging world of modernity, the story goes, new approaches to identity based on formal documents and the related systems for proving identity were therefore necessitated (Bauman, 2004, p. 19). And, thankfully, technologies that could "integrate paper and written records including documentation of identity" were close at hand, following the invention of the Gutenberg press centuries earlier (Chango, 2022, p. 5). It accordingly makes sense to think that the industrialising state might have seized upon these developments to better manage its population.

In the prototypical industrial nation-state, however, this story does not hold water. Whilst Napoleonic passcards had centrally identified French workers in the eyes of the state since 1803, there was never a British equivalent. As Higgs (2011, p. 143) notes, by "the end of the nineteenth century, Britain probably had the most decentralized state in modern Europe"—and, indeed, could be defined by its "relative lack of state identification systems" (2011, p. 110). It is hard not to agree with these conclusions. While the Church, Kings, and their governments would have used many paper-based management techniques to prosecute their affairs, identification systems did not number amongst those tools (Chango, 2022, p. 5). Unlike almost all of their continental European neighbours, the British have never been forced to carry formal identity papers outside of twentieth century wartime. And, even then as we will see, such documents were only briefly tolerated, and swiftly repealed, following the conclusion of each World War (Rolph, 2004). Furthermore, what little personal information the state did hold before the twentieth century was "listed on eighteen disjointed, localized registers" that all-but precluded centralised oversight (EA Whitley & Hosein, 2010, p. 75). The received sociological narrative therefore could, in reality, not be further from the truth. The general presumption in Britain has always been that law-abiding subjects should be left to identify themselves as they see fit, so long as they are not defrauding anyone—a principle that still partly endures today[37].

3.1.2 Negative Liberty and the State

We can begin to understand the deep-rooted aversion to identification in Britain by unpacking where the characteristically liberal will to leave people alone stems from, philosophically-speaking. Much of this was theorised by the Georgians and Victorians, who crystallised the prevailing political thought of their time into concepts and terms we still use today. In general, these theorists understood liberty in 'negative' terms; synonymous with the degree of freedom *from* coercion, obstruction, and interference at the hands of others which an individual enjoys (Berlin, 2002, p. 170). A commitment to negative liberty might mean that I should, for instance, be able to choose how to live without someone else dictating what I can say, what happens to my property, or

[37] There is still no legal requirement to register a change of name in England, though a deed poll can certainly help evidence it.

to which religious or political groups I belong. The more autonomy I enjoy in these respects, the more freedom I could be said to have—and this grants me the space to live according to my own understanding of the good life. As Barry Hindess has put it, Victorian liberalism was thus "commonly understood as a political doctrine or ideology concerned with the maximization of individual liberty and, in particular, with the defence of that liberty against the State" (Hindess, 1996, p. 65). In other words, given the significant capacity that government has to interfere in a person's life—thanks to its extensive powers and agents—it represents a significant possible threat to liberty conceived of in negative terms.

It is John Stuart Mill (1984) who is perhaps most famous for defending this view. His influential harm principle contends that large spheres of private conduct should be placed beyond the reach of society and the state, so long as others are not harmed by that conduct[38]. For many 'classical' liberals, when coupled with a negative conception of liberty, Mill's harm principle consequently outlines the appropriate limits of the state. Governments, they might say, should prevent individuals from harming one another, particularly by upholding the law, but go no further. Through this lens, the British state's historical reticence to identify subjects potentially begins to make more sense. Upstanding members of society would have taken umbrage with attempts to make exercising their freedoms contingent upon state identification, particularly if they were not harming anyone. This was their business, after all, so should be kept free from state interference. And this did not only apply to the upper-classes. Even less well-to-do groups like the "respectable poor" had only to prove locally that they were eligible for relief (Higgs, 2009, p. 350). Neighbourhood identification was certainly necessary to limit fraudulent claims and protect those that were taxed to support the poor, but this did not mean that people needed to be enumerated centrally. As central government did not administer the Poor Laws, it was not to be involved. Keeping these measures decentralised, and thereby helping to defend individual liberty against the state's overreaches, was an important goal for liberals at the time.

3.1.3 Legible, but not Identified

This classically-liberal characterisation of the British state is admittedly neat. But the reality of the subject-state relationship in pre-modern Britain was unfortunately more complicated than the foregoing implies. In particular, the above should not be taken to mean that the state knew nothing about its population, or could not have implemented wide-ranging identification measures should it have so wished. After all, to properly govern a population you first need to know it (Desrosières, 2010, p.

[38] As Mill argues (2003, p. p94), "the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant." We might therefore require licenses for firearms usage, for instance, to head off the harms to society that their unrestricted distribution might lead to.

16)—which is why Scott (1998, p. 2) considered creating a legible population a "central problem of statecraft". And, as we will see, the Victorian's were certainly adept at governing large populations across the Empire, often forcefully controlling individuals via sophisticated identification technologies. At home, however, the approach was always quite different. Rather than identifying individuals, the British state's 'knowing' of its own subjects during this period was instead achieved through macro-level observations of broad demographic trends (Barry, 2020, p. 3). Accordingly, the average Briton would have only rarely showed up as an individual in government records—for instance, in the decennial census, which had been established in 1801 (Higgs, 2001, p. 188). While people were thus certainly made legible to the state, they were rarely positively and individually identified centrally, given how unpalatable this would have been for domestic subjects.

Let me say a little more about the forms of legibility to which Britons were subjected. In addition to the census, the main records of personal information at this time could be found in some of the earliest civil and military registers. Since 1837, for instance, the General Register Office (GRO) had administered the civil registration of births, deaths, and marriages to make up for the failings of the old parish-based system in England and Wales[39]. National policymakers no doubt occasionally drew on this data, even though the GRO was primarily formed for "medical scientific purposes" and to support "local government" decision-making (Higgs, 2001, p. 180). But, although the scope for centralised surveillance of individual civilians via their birth or marriage certificates was effectively nil, as these documents played no role in the day-to-day identification of individuals, some subjects of the Crown were tracked more closely. In particular, pay lists, musters, and pension records—for both active and retired servicemen—had been well-maintained by the Admiralty and War Office for well over a century (Higgs, 2001, p. 178). These military records are therefore likely "the oldest form of personal archival file" in Britain (Macdonald & Lenihan, 2018, p. 376). However, while such files accounted for the movements and status of servicemen, they, too, did not amount to identity documents. Individuals remained responsible for identifying themselves to others, without recourse to such records, let alone evidence like identity cards or dog-tags.

There are other reasons the state may have opted to govern in this manner at home. After all, communications at the time were slow; limited by the speed of men and horses. And the then-nascent discipline of statistics—which can literally be read as "state-istics", or the science of the state (Schmidt, 2005, p. 15)—essentially relied on data recorded locally, on reams of paper by clerks, which would then later be pooled centrally and transported to statisticians for analysis. Information therefore mostly flowed one-way, slowly, up the chain, providing limited scope for central state administrators to directly interfere in subjects' lives on an individual level. While one

[39] The Scottish equivalent was setup in 1854.

could consequently suggest that this was an intentional choice, to insulate subjects from interfering Whitehall bureaucrats, to do so would be misleading. As we will see, favouring statistics over identity systems did not in fact preclude the state's often-extensive interference in peoples' lives; it just ensured that such management occurred at a demographic, rather than individual, level. Indeed, collecting statistical data on the domestic population became essential to pursuing several quite invasive projects of societal improvement during the 1800s, as well as measuring such the success of such projects. And these methods proved quite sufficient for attaining the legibility required for the state to pursue its goals—rendering the implementation of more granular identification systems simply unnecessary.

3.1.4 Positive Liberty and Societal Improvement

What drove these Victorian projects to improve Britain? Politically, motivation stemmed from a growing recognition that excessive respect for individual negative liberty, and especially private property rights, had failed to create a stable and fair society, systematically disadvantaging vast swathes of the population (Freeden, 1986). Especially via the influential work of T. H. Green, a 'new liberalism' was accordingly synthesised in the late-Victorian era. Responding to classical liberalism's more laissez-faire tendencies, new liberalism instead promoted the need for social and economic reforms to help alleviate material inequality—employing what we would now recognise as a far more 'positive' notion of liberty (Duncan Bell, 2014, p. 700). Above all, this meant that people would need to discover their own "'real', or 'ideal', or 'autonomous' self" , and so be freed from "irrational impulse" and "uncontrolled desires" (Berlin, 2002, p. 181). Most offensively for classical liberals, this would require the construction of extensive state apparatuses around the provision of social welfare, to realise better education, material redistribution, and improved physical health. Consequently, as Michael Freeden (1986, p. 53) puts it, "the ideological history of the nineteenth century should be depicted as a constant encroachment of the idea of welfare (material and other) on the idea of freedom from intervention".

By the end of the century, the British state had accordingly developed various disciplinary techniques intended to address a wide variety of these social ills, all tracked via new programmes of statistics (Rose, 1999, pp. 103–105). Taken together, these Foucauldian developments changed the relationship between subjects and the state. In particular, the latter's growing usage of 'technologies of observation' to make individuals legible and ensure individuals would be sufficiently educated and materially supported had "created new mechanisms for the production of social and political order" (Gorski, 2003, p. xvi). Recording the relative levels of education and illness, for instance, allowed the state to respond, creating a steady supply of reasonable, civilised, and healthy workers. The development of public spaces—policed for safety and made hygienic via sewers—also provided room for personal growth and enjoyment, in line with strict social mores that would be enforced via social observation. And prisons, workhouses, and sanitariums would contain and

attempt to reform those that did not, or would not, conform. From the classical liberal's perspective, all of these interventions, devised and tracked via statistics, would thus have been seen as fundamentally oriented towards the often-paternalistic interference in subjects' lives; favouring one particular vision of 'freedom' that not all would have found agreeable.

Understandably, this did not sit well with classical liberals. The coercion of individuals that welfare reforms had required was anathema to a liberalism that had strived to leave each to his own ends. Nonetheless, the 'new' liberal movement continued to build, reaching its peak in the wake of the World Wars. And not only were various new liberal institutions intimately tied up with efforts to make the population more legible—and later identifiable—to officialdom, but it was only through later identity systems that many social interventions could be realised in the first place (Lyon, 2009, p. 36). Understanding this will consequently help nuance our evaluation of Britain's development of state identification measures, as the state's actions over the past century or so present an interesting case study through which to evaluate the influence of these two notions of liberty. As we will see, technological developments that had been honed during the Industrial Age, particularly abroad, made people progressively more knowable to the state bureaucracy at greater levels of granularity during this period—beyond the general level of early statistics. And the centralised knowledge gathering, and even surveillance, that identification entailed—part and parcel of the power to dominate through bureaucratic means (Weber, 1978, p. 225)—was a necessary precursor to the more precise state interventions that characterise much modern social policy today. It is thus to these wartime developments that we will now turn, to evaluate just how dramatically they deviated with the past.

3.2 Passports on the Eve of War

If, for most of British history, the average subject had lived a life largely unencumbered by formal, centralised state identification systems, then how did this change during the early twentieth century? Most obviously, Whitehall dramatically escalated its identification practices in this period—albeit later than many other industrialising countries. In doing so, the state began to move beyond the observation of legible *populations* to embrace positively identified *individuals*. This happened contiguously with the formation of the recognisably-modern nation-state, as Europe prepared for war; with countries solidifying their borders against a backdrop of the mass migration of refugees and soldiers (AJP Taylor, 1965, p. 2). Today, political scientists consequently recognise that one of the central characteristics of modern statehood is the state's ability to define its citizens—not only distinguishing members of one's own society from others, but also controlling the passage of individuals into and out of one's territory (Dryzek & Dunleavy, 2009, p. 3). But, in the early 1900s, this was a novel task for a civil service that had little experience identifying anyone within the country. Nonetheless, on the eve of war in Europe, centralised identification

systems were finally introduced—first at the borders, then in the streets. This would spell big changes for those living and working in Britain, further altering the relationship between the people and the state.

3.2.1 Identification at the Borders

Today, both international travel and proving one's citizenship are synonymous with the presentation of a passport. But passports as we know them today are actually a very recent innovation. It is for this reason that sociologist John Torpey (2000) has identified the establishment of the global passport system in the early twentieth century as such a pivotal a moment in the history of the state. In particular, Torpey locates the "monopolisation" of citizens' "means of movement" via passports as an essential feature of their "development *as* states" (Torpey, 2000, p. 3). This is because modern passports, along with the border management infrastructures they rely upon, affirm the primacy of the nation-state as a political unit. They depend on the mutual recognition of, and cooperation with, other states, while making the ability to both travel internationally and claim a formal identity whilst travelling contingent upon belonging to a particular state. This further downplays the importance of identity performances. In turn, it also makes exercising certain forms of liberty newly-dependent upon bureaucratised, technical processes of identification and identity-checking carried out at the borders, forging a link for the first time between citizenship and such 'rituals' of identification (Torpey, 2000, p. 4). The modern passport is consequently emblematic of a significant rupture with the past. And it was via the passport that most British subjects first encountered the reductions in personal liberty that identification systems can engender.

Passports, it is worth pointing out, were not a new invention in the early 1900s. They had existed in some form or another in Britain since at least 1414, yet would not be treated as national identification documents until half a millennium later (Higgs, 2011, p. 156). These early ancestors of the passport also had little in common with their modern equivalents. Rather than functioning as permissions to cross the border, historical passports instead marked the holder out as being under protection of a monarch when travelling abroad (Lloyd, 2008). They were thus certainly not required for travel in the eyes of the British state—no one would have checked them when entering or leaving Britain—and were given to allied nationals *and* foreigners alike, as the monarch pleased, to help ensure their safe passage in foreign lands (Higgs, 2011, p. 112). Well into the nineteenth century, passports were in fact only required when travelling through the few countries that mandated such nuisances, like France (Chango, 2012, p. 214). Accordingly, "the system was generally reviled by the public" in Britain, not least for the implicit doubt it cast on the character of those people who could afford to travel internationally, and who did not believe they needed documents to prove who they were (Lloyd, 2008, p. 6). Most people therefore simply did not bother to apply for a passport and travelled anyway, particularly if their trip did not

pass through countries that required them. Again, the British penchant for the laissez-faire can thus be recognised here—especially amongst the wealthier classes.

But, perhaps surprisingly, this general lack of a requirement for state identification at the borders did not only apply to British subjects at the time (AJP Taylor, 1965, p. 1). Foreigners, too, were entirely unencumbered by passport requirements. In fact, until the eve of the First World War, the movement of aliens into and out of Britain, as well as within it, had been to all extents free; no passports had been required to enter the country for the past several hundred years (Higgs, 2011, p. 112). Additionally, the few decrees which had in the past restricted the movement of foreign merchants, traders, and visitors—requiring them to register at ports and pay double taxation—had been repealed a century earlier during the early-Victorian era, along with unrelated laws that had ineffectually attempted to control the movements of the very poorest Britons between pre-Modern serfdoms (Torpey, 2000, p. 67). The turn-of-the-century British state could accordingly be defined by its laissez-faire attitude to migration and travel both internally and externally, likely due in part to its lack of a land border with mainland Europe. To take a further example: following the Act of Union in 1800, large numbers of Irish workers had moved to the north of England and, along with many other jobless Britons, simply emigrated to North America without any state oversight of their passage (Torpey, 2000, pp. 67–68). The British information state plainly did not worry about tracking these kinds of movements, even though many of its European neighbours would have gone to great lengths to record such persons.

So, at the dawn of the twentieth century, central government had a very limited view of who most individuals within its borders were, where they were from, or where they were going. It is consequently no surprise that Torpey attaches such weight to the introduction of the modern passport system in the years immediately preceding the First World War. Passports were completely reimagined—from a personal vouch from the monarch to a legal requirement for foreign travellers. Visitors' movements were severely restricted via these new controls, reducing their liberty while subjecting them to "documentary surveillance" on previously unseen levels (Torpey, 2001, p. 257). This was a dramatic reversal of the state's previously-liberal approach. And passports were only the beginning, as the state soon deployed other forms of documentary registration to control and surveil foreigners' movements. What is more, the impetus for these policy changes was characteristically illiberal—fundamentally motivated by racism; a way to separate 'them' from 'us'. In particular, Eastern European Jews had begun immigrating to Britain in large numbers as war loomed. The Aliens Restriction Act of 1914 had therefore harnessed growing antisemitic sentiment amongst portions of the public to place new requirements on anyone who did not "look or sound 'British'" to prove their nationality and, if they were foreign, to register their movements with the authorities (Torpey, 2001, p. 258). Britain's days as a laissez-faire, cosmopolitan mixing pot were accordingly over.

As often happens, these controls were also only meant to be temporary and limited. But the Aliens Order of 1920 extended them to apply to any traveller, foreign or domestic (Torpey, 2001, p. 263). The shift in freedoms that British nationals faced after the First World War was thus stark. Submitting to formal identification while travelling was no longer a choice, backed by monarchical privilege, but now mandated. And, not only were Britons compelled to carry and present documents for the first time, but their prima facie right to access foreign territories was lost (Torpey, 2001, p. 269). Although British subjects were affected, however, I must reiterate that the burdens of these new controls were not equally shared. The most invasive requirements applied to foreigners alone, effectively creating a two-tiered society. Whilst British subjects certainly faced the newfound inconvenience of having to carry a passport, replete with their photograph or other proof of identity, they were still mostly free to move as they liked. Aliens, on the other hand, were recast as 'other' and subjected to newfound enumeration, tracking, and controls both at and away from the borders. This included the establishment of a central register of foreigners, through which people's movements could be recorded and corroborated with the help of private surveillance sourced from innkeepers and other informants—massively impacting their privacy and freedoms, and denying any notion of equality with British nationals (Torpey, 2001, p. 263). Such methods had never before been instituted, and were accordingly accompanied by a dramatic expansion of the immigration bureaucracy.

3.2.2 Despotic vs. Infrastructural Power

One way to understand these radical developments is via two interlinked conceptions of power that sociologist Michael Mann (1984) has termed despotic and infrastructural. On the one hand, despotic power refers to the centralised, coercive ability of monarchs, rulers, and lawmakers to act without institutional constraints. In political-philosophical terms, we might accordingly think of the Hobbesian leviathan, looming over his territory. This notion captures how despots can act according to their own whims, without considering the interests or input of others in civil society, and exercise their authority via force, fear, and coercion rather than consent. Infrastructural power, on the other hand, refers to the capacity of a state to logistically manage its territory and implement its actions through procedural means. In political-philosophical terms, we might think of Foucauldian disciplinary forms. This concept of power arises from the state's ability to build-out infrastructure that penetrates and embraces society, like transportation networks, communication systems, and bureaucratic administration schemes. It therefore depends on cooperation and coordination between the state and civil society groups—power that stems from consent and capacity rather than just coercive force. Most states, Mann thinks, can consequently be described by the relative levels of despotic and infrastructural power that they exercise; and Britain is no different.

Before the nineteenth century, for instance, passports were the perfect illustration of despotic state power. British monarchs marked out those worthy of their protection while abroad, and personally vouched for their safekeeping through the projection of their absolute power across various territories and alliances. But this meant their holders had to be known (at least loosely) to the monarch, or else could gain access to them through personal networks. This practically limited the acquisition of passports to the elite. The large scope for bias and discrimination at play in such a system should be obvious, and was only compounded by the arbitrariness of the power which the monarch wielded; at any point, their vouch could be withdrawn. And, while George III stopped personally signing passports by 1794, making them then somewhat easier to acquire, any potential traveller would still have needed to "either know the Foreign Secretary personally, know someone who did or have a recommendation from a banking house of repute" (Lloyd, 2008, p. 10). Passports were consequently overwhelmingly held by the well-to-do in society before the First World War, with their acquisition tied directly to the despotic power and whims of some of the most senior members of British society. Rather than an imposition, they were marker of personal status, standing, and power. They did not reduce, but extended, the freedoms of those few Britons lucky enough to possess one.

The new passport system, by contrast, replaced the arbitrariness of the monarch's favour with the rigid mechanisms of an informational bureaucracy. Passports now also constrained, rather than enabling, liberty. This was why the French had vigorously resisted their normalisation, over a century earlier, as they thought making travel contingent upon such systems directly undermined their natural and civil rights (Torpey, 2000, p. 22). In some ways, though, the new system could also be praised for being more equal. Although it made international freedom of movement newly-contingent upon the presentation of documentary evidence, at least all travellers were now required to carry passports, as they would be demanded throughout much of Europe and the West (Lucassan, 2001). But while procedurally administered in a fairer manner, the new system was also unfair in a fundamentally deeper way; motivated by a desire to exclude certain groups from the political community. This reflected the disturbing ethno-nationalistic forces spreading throughout Europe at the time. And, to support the logistics of such a totalising system, immigration infrastructure also newly permeated the entire country—not only at the borders, but inland through the distributed networks of informants and immigration officers. The state thus diffused its infrastructural power through the countryside and cities, monitoring those that were admitted in case there was cause to eject them at a later date. All of this made a large number of people knowable to the state that had never before been tracked in such detail.

3.3 Wartime Identity Cards

Passports, however, were just the beginning. The British state's infrastructural power was now in its ascendency—and, as the threat of war grew, government took

further "political actions that would have been unthinkable before 1914" (Agar, 2001, p. 103). Beyond tracking foreign nationals, developments during the Great War like rationing, conscription, requisitions, and the later expansion of the franchise would all rely on gathering "information on the population at an individual level" in newly centralised registers (Elliot, 2006, p. 146). Consequently, the state's primary producer of information, the GRO, would slowly transform from its previously limited role into "a true system of state surveillance" and personal identification (Higgs, 2001, p. 185). Records of the name, age, location, and employment of almost every adult citizen in the United Kingdom would be documented by local clerks and compiled in the National Register (NR) to facilitate National Service and other war work, with individuals obligated to keep the state abreast of any changes to their personal situation (Agar, 2005). Far more than just being made legible, all people living in Britain—foreigners and nationals alike—were thus to be positively identified and surveilled in a system that fed directly into the machinery of central government. And it was only thanks to the risk of total warfare, and later promises of 'total welfare', that this dramatic growth in information collection, processing, and utilisation was legitimised and tolerated (Higgs, 2004).

For individuals living through the First World War, the most obvious expression of these changes was not to be found in the establishment of the NR itself, but rather the associated physical identity cards that subjects were ordered to carry. These cards essentially functioned as proofs of entitlement, fixing an individual's identity via documentary evidence (Lyon, 2009, p. 6). Nothing like this had ever before been imposed on normal, law-abiding subjects. Analogous to 'internal passports', identity cards too relied on systems for checking identities and eligibility at checkpoints. Their full adoption could therefore again have extended the sphere of suspicion surrounding individuals in Britain, further impinging upon their liberties away from the borders. While passports were only checked at ports, identity cards could in theory be demanded by the authorities from anyone, anywhere; whether accessing a service or simply due to 'suspicious' behaviour. If such checks had become commonplace, they would consequently have cemented the state's control of its population, foreign and national, by diffusing identity checking infrastructures throughout Britain. In reality, though, this actuality never materialised. As Jon Agar (2005) has noted, once the initial registration drive had allowed the government to calculate the number of able-bodied men available for National Service—the policy's real purpose—the cards were all-but abandoned. Agents of the state did not in fact regularly check them, and nor were they used to control access to services.

Liberty for those who were not called up consequently was not, as feared, made dependent upon submitting to this new form of infrastructural power. The state did not, in fact, embrace the population via a totalising system of population management. Instead, cards were usually "lost, left in pockets and the backs of chests of drawers" (Agar, 2005). One reason for this is that the cards were relatively crude and recorded only the holder's name, ID number, and address. They were consequently not overly

useful to the authorities, who did not see the point in checking them (Agar, 2005). Without a photo, or even a signature, cards did little to prove someone was claiming their rightful identity—unless the individual was already known to the official in question. But, despite what the public may have thought, it was not the cards themselves that would necessarily have resulted in the greatest changes for their relationship to the state. Unbeknownst to most, the GRO was also simultaneously filing the information recorded on the cards, and more, centrally, in the NR's transcript books. Dossiers on normal people in Britain were, for the first time, therefore being made individually intelligible to the central state bureaucracy, so that it could respond and act (Scott, 1998). And it was these records that had the potential to truly alter how the state operated, offering civil servants a novel way to join-up departmental silos across Whitehall using individuals' ID numbers (Rose, 1999, p. 131).

Despite the "dismal failure" of identity cards in practice, concerns about the general trajectory they indicated consequently did not abate (Elliot, 2006, p. 151). In particular, the significance of the NR was not lost on politicians. As Agar (2001, p. 102) has elsewhere argued, "[i]n peacetime, partial systems gave the appearance of liberty—and therefore distance from continental models". Much like a constitutional separation of powers, the lack of universal ID numbers had limited the scope for central, surveillant oversight. But this well-understood administrative friction had proved too inefficient to retain during wartime. It was thus alarming for classical liberals to learn that records across different departments were starting to be connected up in the background via ID numbers, despite the threat to civil liberties some believed this posed (Higgs, 2001, p. 185). During fierce parliamentary debates, MPs therefore warned of 'Prussianism', and identified the NR as "an interference with the customs and liberties of the people unparalleled in the history of the country" (*Hansard, HC Deb vol 73 col 108*, 1915). Together with new liberal redistribution, the war had already precipitated an unprecedented enlargement of the state. Additionally, MPs feared the register would be used to compel conscription—negating individual autonomy by undoing the traditionally voluntary basis of recruitment. Pro-NR politicians accordingly countered by linking patriotism to wartime registration, with sceptics accused of "opposing the war effort" (Elliot, 2006, p. 151). Citizenship and the possession of formal identification were thus further conflated.

In the end, of course, the threat of losing freedom tout court—should the war be lost—had won out. And, for a brief moment, the move towards central oversight, and possible interference, via identity cards certainly seemed well-tolerated—even if the cards were not used much in practice. Were the new liberals therefore winning the argument? Statistics and demographics were, it seemed, being well and truly superseded; supplanted by individual-level enumeration that could, in theory, be used to track individuals across all their interactions with the state. Combined with the perceived competency of Britain's management of the war, classical liberals' arguments around undue paternalism had thus seemingly been undermined—not least because, to many onlookers, government had become "more genuinely the

government of the people by the people themselves" in the preceding decades (Ritchie, 1896, p. 64). Would people therefore willingly submit to centralised identification, so long as it was led by a democratic government? The answer was a resounding 'no'. Even though some civil servants wished that the "the national registration system be continued", the need for these exceptional restrictions had now abated (Elliot, 2006, p. 151). Following the Armistice, identity cards were soon repealed due to "public anxiety" over "state interference" (Elliot, 2006, p. 151). The short-lived experiment in centralised identification was consequently over, at least for now, and the decentralised status quo resumed. Life in Britain had not yet become dependent upon documentary checks.

3.3.1 Identity, Home and Away

The wider point here is that identity systems of many different stripes have always been a hard sell in Britain—at least on home soil. Partly this was due to the deep-seated cultural suspicion surrounding certain identification technologies. Biometrics, or bodily identification techniques, were especially mistrusted, as they were deeply tied to wrongdoing and criminality in the national psyche. For hundreds of years, criminals, fugitives, and vagabonds had been branded, cut or burned to mark them as "deviants"; and tattooing, which was associated with military desertion, had an equally terrible public image[40] (Higgs, 2011, p. 89). Bodily markings were therefore not considered an appropriate method for identifying British subjects. Even techniques that relied on reading features off the body, rather than marking it, were unpopular. Fingerprinting, for instance, which Imperial civil servants had used in India since 1858 to identify colonial subjects and get them to 'sign' contracts and deeds, was only adopted by the Metropolitan Police in 1902 (Sengoopta, 2004). And the Met approved fingerprinting for criminal identification purposes alone, despite other possible uses, with early attempts at identification via facial measurement likewise reserved for criminals. Although the police knew these techniques could have helped identify missing persons and the dead, they were wary of any perceived criminalisation of law-abiding Britons[41] (Higgs, 2011, p. 89).

---

[40] This did not deter firebrand philosopher and social reformer Jeremy Bentham from trying to make the tattoo part of everyday life. He contended that proper names were not fit for purpose, and instead argued that every individual should be tattooed with a unique identifier (Caplan, 2001, p. 107). Amazingly, to help popularise his plans Bentham even tried to get members of the upper classes to tattoo their titles on their foreheads (Higgs, 2011, p. 77)—an idea that, unsurprisingly, did not catch on. Instead, and surely much to his annoyance, the English remained satisfied with their traditional and relatively imprecise means of identification based on personal relationships.

[41] For similar reasons, Treasury proposals to fingerprint welfare claimants were abandoned in 1921 due to insufficient interdepartmental support (Higgs, 2011, p. 144). Yet, in some cultures, such systems have been observed for millennia. Thus, in China, there is ample documentary evidence dating from as far back as the Qin and Han dynasties (221 BCE–220 CE) of state officials using handprints and fingerprinting for personal purposes.

As these examples suggest, however, the British state had still played a key role in developing novel identification technologies. It was just confined to testing them abroad to avoid upsetting its domestic subjects. Identity cards, for instance, had been used to manage populations throughout the Empire for centuries before their first aborted introduction at home—and would continue to be used for decades to come. Such systems helped colonial officials segregate subjects, differentiating between the oppressors and oppressed. In South Africa, a combination of 'pass laws' and simple paper identity documents had, since 1760, severely restricted the freedoms of the non-white population[42], facilitating the arrest and prosecution of nearly 18 million South Africans over a 70-year period (Savage, 1986, p. 181). And, after the election of the National Party in 1948, identity cards would continue to underpin the administration of apartheid (Breckenridge, 2008, p. 41). Similarly, in Hong Kong, identity cards were introduced in 1949, initially to control immigration from mainland China. But, by 1980, anyone in the territory who could not produce a valid card when challenged was to be deported, regardless of origin. Clearly, when it came to foreigners, the British state had no trust for many of these communities. So, while the state knew such systems would not have been accepted on home soil, it happily deployed identification technologies abroad to manage the 'unruly' other[43] (Lyon, 2009, p. 35).

Like passports, identity cards consequently advanced the displacement of identity performances for identification purposes. Across the Empire, the British state had, for decades, favoured formal methods of identification that lent themselves to bureaucratic evaluation, and wrested the means of identification from foreign populations so that it could set its own terms around how and when an identity could be proved, and any associated entitlements enjoyed. These systems handed bureaucrats power to effectively subvert equality, subdividing and controlling populations. Sociologist David Lyon (2001) has accordingly identified such 'social sorting' as a primary purpose of identity systems. He highlights the ways in which various identification and surveillance technologies have been used to make decisions about individuals and groups throughout history. In doing so, Lyon (2002) draws attention to how such systems often reinforced existing social inequalities and power structures. For instance, to the British state, "Catholics were suspect, as were peoples from colonies in India or Africa", so—as we have seen—identity systems were used to distinguish "between legitimate and illegitimate identities" and restrict the freedoms of the latter (Lyon, 2009, p. 36). The same social sorting techniques had not yet been rolled-out in Britain, though. The question, then, was if the civil service would ever again try to employ similar mechanisms to manage the domestic

[42] Whilst certainly not equivalent, paupers in England had been made to carry similar documents for crossing the borders between counties in the medieval period (Higgs, 2004).

[43] It was only thanks to Britons' cultural mistrust of bodily identification that wartime identity cards had not carried photos or fingerprints. Cards containing only minimal information preserved the veneer of acceptability just enough to make them tolerable for the duration of the war.

population, building on its brief attempts to centralise identification during the First World War.

3.3.2 The Second World War

Sympathetic civil servants had not given up and, while they bided their time, ensured they had detailed plans ready for their next stab at rationalising the state bureaucracy (Higgs, 2004, p. 137). Two decades later, as the Second World War loomed, officials were therefore quick to reintroduce an enhanced version of both identity cards and the centralised register, with their social sorting objective now made far more evident. Again, subjects would have to submit themselves to registration, and report changes of address to support the war effort—despite the fact that the surveillant effects of constant reporting were one of the chief concerns the public had raised during the First World War (Elliot, 2006, p. 152). To guarantee adherence, and counter this resistance, the state therefore constructed various useful purposes for the cards. Everyday tasks, such as making passport applications, opening and accessing Post Office savings accounts, collecting parcels, and claiming rations, were all made contingent upon the presentation of an identity card to officials. Such "entitlement" and "compulsion" were thus key aspects of the reintroduction (Elliot, 2006, p. 176). And, given that cards were made "essential", it was no surprise that "people cooperated with the system, and the Central Register was well maintained" (Agar, 2001, p. 109). There was, after all, no legal way to buy food and live a normal life without submitting.

As mentioned, the new cards also made their social sorting effects particularly apparent. The sense of 'them' and 'us' was notably deepened, not least because cards were vital for separating "eligibles from ineligibles" in the context of British jobs and access to the wartime welfare state (Torpey, 2001, p. 270). Most obviously, a card's colour clearly telegraphed the socially-stratified group to which an individual belonged. While the first batches of cards were initially all the same shade of brown, later changes visually distinguished different levels of entitlement and belonging (Thompson, 2008): government employees, for instance, held desirable pink cards, essential workers with access to war-sensitive areas had green cards, whilst temporarily-admitted Irish workers were picked out by yellow cards. Both contrasted with the blue and brown cards that most British adults and children received. These changes consequently took a population that had previously been all-but unknown to the state on a personal level, to an enumerated, subdivided, and individually-identified collection of people—each entitled to different levels of state support—that would regularly have to prove who they were as well as their eligibility. Accordingly, this "new knowledge regime created a novel political capacity in the state", oriented around the bureaucratic production and checking of identification (Mukerji, 2011, p. 225); an impressive about-face for a government that had, until recently, shown little interest in instituting such methods of governing at home.

Several advances made under this new knowledge regime related to the technological affordances of the cards and the register behind them. For instance, the new universal IDs encoded detailed information about where someone was from, their position in the household and, in some cases, extra details (such as if they were a diplomat) to help central register workers better manage the scheme (Thompson, 2008, p. 148). More obviously, to better bind documents to their owners and prevent fraud, cards now featured signatures, which could be checked against those held centrally if a replacement was requested, along with various other datapoints (Higgs, 2011, p. 155). Cards were also stamped, which made them harder to fake (Thompson, 2008, p. 149). And cards for government employees and essential workers went beyond signatures, with photos of the individuals in question affixed to their front (Thompson, 2008, p. 151). These developments reflected the growing technological capacity of the state to innovate around identification. But, on a political level, they also further socially-stratified the population. So desirable were pink and green cards that some people manually added photographs to their blue cards to try and garner the "favourable treatment" that those cards' holders received (Higgs, 2011, p. 155). By contrast, cards that picked out aliens subjected their owners to greater stigma and stricter surveillance (Thompson, 2008, p. 155). And, of course, documents were also regularly checked across everyday life, as agents of the state could request them at any time. Social sorting, enabled by identity cards, was now alive and well in Britain.

It is also worth stressing that the register and identity cards were not just a wartime necessity. The new system was explicitly intended to alter aspects of the subject-state relationship in Britain. Social reformers Beatrice and Sidney Webb, for instance, saw the register "as a means of social control and promoting the rights and responsibilities of the citizen" (Elliot, 2006, p. 170). They had therefore worked with other enthusiasts to refine government's plans in the interwar years, and viewed both the register and cards as essential to the promotion of positive liberty under the welfare apparatus—both as a source of data about the population, to guide reforms, and as a tool through which to pursue redistribution. The main way this manifested was via rationing, whereby freedom and autonomy—especially in the formal market—were made dependent upon the presentation of valid identification. Without a card, a ration book could not be acquired, and access to the state-controlled food supply would be denied (Agar, 2005). Government therefore asserted power to dictate how much people ate by tying rationing to the implementation of centralised identification, exerting deep control over this and many other facets of normal life[44]. And so effective were the system's compulsive effects, thanks to this setup, that the central register outperformed all expectations—Higgs suggests that the

[44] Away from the borders, community had still reigned supreme for identification purposes until the outbreak of war, with trusted officials and respectable professionals expected to countersign and vouch for state benefits, pensions, and passport applications (Higgs, 2011, pp. 148–149). But now formal identification was necessary to even subsist.

"thoroughness and universality of the resulting identification system exceeded that created in the totalitarian regime of Nazi Germany" (Higgs, 2011, p. 154).

The system's influence was not constrained to the food supply alone, however. By the time the war was won, a huge list of government services relied on the register, thanks to function creep: "health, insurance, immigration, voting, policing, refugee control, mercantile marine identification, internment, pensions, population statistics, birth, death and marriage recording, and so on" were all tied to a person's universal ID numbers in the background, and the presentation of an identity card at the point of service (Higgs, 2011, p. 155). The whole system was consequently antithetical to "the idea of liberty as freedom from the State, rather than through a State" (Higgs, 2011, p. 156). By pushing such a positive conception of liberty, for good reasons and with the general consent and cooperation of the population, the freedom to exist without state identification had been well and truly removed in many contexts. Again, however, this had only been tolerated for exceptional reasons. With the threat of Nazism dealt with by 1945, pressure thus soon mounted to reverse the statism of the war effort. And, in 1952, the programme was scrapped—famously precipitated by the actions of a young liberal, no less, who objected to a policeman demanding to see his identity card when caught speeding (Agar, 2001, pp. 110–111). Although public sentiment had long since turned against the system as a whole, this well-publicised event was the final nail in the coffin (Thompson, 2008, p. 157). Again, the state had failed to justify the need for such a totalising system in peacetime.

3.4 Postwar Welfare and Computerisation

While the unacceptability of centralised state identity systems had once again been reasserted, however, the concentration of the state more generally would continue—helped along by growing adoption of a nascent technology. In particular, the postwar period witnessed a significant expansion of the central welfare state in Britain (Nullmeier & Kaufmann, 2021). There were several reasons for this. Following hard-won victories in two World Wars, trust in government was running relatively high, with successive reforms perceived by many to have further lessened (but by no means eliminated) the sway that a self-interested ruling class had previously held over politics (Wolff, 2015, p. 366). Nevertheless, while citizens[45] may now have enjoyed equal civil and political rights on paper, the reality of pervasive and severe economic inequality in the postwar period was still seen as unjust—particularly after so many had lost their lives fighting to defend the liberal democratic order. Further redistribution was therefore considered necessary to promote material equality in addition to equal basic freedoms for all. Consecutive governments pursued new liberal policies oriented towards realising this Keynesian end, pushing for full employment, a mixed economy funded through progressive taxation, and an

[45] As detailed below, subjecthood was replaced by citizenship following the war.

expanded welfare state (Addison, 1994). Despite the fact that citizens and residents were no longer required to carry identity cards, the effects of centralised management techniques therefore continued to be felt.

There is much to unpack here, but only two interlinked aspects of these developments are relevant for our purposes—the computerisation of the growing welfare state, and the cooperation between the state and private companies that this relied on. First, though, it is important to acknowledge just how radical the project as a whole was. Building on the National Insurance Act, the Beveridge Report (1942) had outlined a visionary system of national welfare, based on compulsory social security. When the Labour government implemented Beveridge's plans in 1945, the modern welfare state was consequently born, amounting to the largest centralisation effort Britain has ever undertaken. From newly-defined rights flowed citizens' entitlements to never-before-seen state benefits and services—with the most dramatic of these primary goods being free universal healthcare under the National Health Service (NHS) (Kuhnle & Sander, 2021, p. p89). In philosophical terms, a new social contract between the people and the state had thus been struck, justifying the civil, political, and social rights that still motivate public services provision today (Lips, 2006, p. 35). But achieving this would be a mammoth administrative undertaking, requiring a "vast technological network that undergirded what the British government provided to all of its citizens" (Hicks, 2019, p. 22). Officialdom therefore leapt at the opportunity to enhance its paper-based bureaucracy with a new technology, computers—the last piece of the puzzle we must prise from our evaluation of historical identification systems.

3.4.1 Hollerith Machines

Key to many increases in legibility, surveillance, and welfare across much of the Western World over the latter half of the twentieth century has been the adoption of computerised systems, built on taxonomies that could bring order to ever-greater amounts of information (Hicks, 2019, p. 23). Much of this information processing capability was developed not by the state itself, however, but by private companies. The principle example has to be the punch-card tabulator systems—Hollerith Machines—developed by the company that would later become International Business Machines, or IBM (Black, 2001). Originally designed in the 1880s to help record the US census, over the next hundred years these electromechanical devices would precipitate a revolution in data processing the world over, impacting the lives of millions. This was because, compared to manual recording, calculation and sorting, electrification realised a step-change in processing capacities. Hole-punched cards could be read by the machines incredibly quickly, to support statistical calculations and data management tasks. And, while certainly not equivalent to modern data-based computers, which operate digitally, these analogue computers still revolutionised the centralised information state (Hicks, 2019, p. 23). The automated and semi-automated processing of data was an essential technological advancement

for growing the state bureaucracy, building on a groundwork of general literacy amongst administrators.

As we have seen, however, greater legibility comes hand-in-hand with the potential for oppression, particularly when coupled with a state's untrammelled coercive power. And early computers were no exception. Beginning in the 1930s, IBM had nurtured a direct collaboration with the Nazis—first to support a national census, then to help identify, numerate and track Jews and other minorities during the Holocaust (Black, 2001, p. 198). Indeed, IBM's machine-readable identity cards were essential for administering the genocide; every concentration camp had its own Hollerith Department (Black, 2001, p. 351). Right from the beginning, then, computerised identification technologies were bound-up in one of the most appalling atrocities in human history—and not just as an incidental administrative tool. While the National Socialist ideology dehumanised its victims, the act of computerisation played a part here, too. By abstracting away from the people involved, reducing them to hole-punches on a card, computers contributed to the de-personification of humans during the Holocaust[46]. After all, strings of unique identifying numbers—which, in the Auschwitz camp, were even tattooed onto prisoners' bodies—could be manipulated as 'just' entries in the machines, alienating administrators from the very real people and actions that resulted from their decisions. And, while this administrative distance certainly did not reduce the moral culpability of those involved, in a Arendtian manner it does suggest how making evil acts banal, via computerised abstraction, made them easier to plan (see Arendt, 2006).

Right from the start, computers therefore displayed a deeply troubling potentiality for alienation. Yet despite its complicity with the Nazi's, IBM faced no repercussions after the war—and continued to sell computers. The boost in administrative power that electromechanical processing gave bureaucracies was simply impossible to ignore, and other governments were already using the very same devices; the British civil service had quickly adopted Hollerith Machines along with most of Europe and America (Higgs, 2004, p. 147). No more would clerks need to manually tabulate and calculate figures, limiting the scale of the state's ambitions. Records on entire populations could now be processed, centrally and efficiently. As we will see, this made computers essential for the rollout of National Insurance and the postwar welfare apparatus in Britain (Hicks, 2019, p. 23). Without computing, these reforms would have been far more difficult to institute. But, at the same time, computers no doubt also further devalued the importance of identity performances

[46] This point was forcefully put to me by Phil Booth, a privacy researcher, who shared his experience of meeting a Holocaust survivor in the East End of London. Booth recalled how the man "had his fucking tattoo on his arm, and held my hands and said, 'you just can't let them turn people into numbers, because it ends in the ovens'." Although he recognised that "some people say that's extreme […] it is a real thing when you start to put a number on a person and the system starts to treat people as numbers." I hope to have captured some of this sentiment in the main text.

between individuals. It is consequently hard, if not impossible, to not see computerisation as a pivotal step in the advancement of identification systems, and the development of the modern administrative state. This is despite the fact that, as more powerful electronic (rather than electromechanical) computers later proliferated, the alienation they can engender from the historical sociality of identity would persist—with all the associated problems this could raise for the people the technology would increasingly be used to administer.

3.4.2 Computerised Identification Practices

As examples throughout this chapter have shown, the values at stake in state identification are complex and multifarious. But even the earliest computers seem to have qualitatively changed something about how the state went about identifying people—and there is, of course, more to say about this in future chapters. At the same time, though, computerisation also simply deepened the already considerable discriminatory power of traditional identification systems, by boosting the scale and complexity of processing that was possible. In doing so, this placed citizens at greater risk of unwarranted control and exclusion. But we must be careful here. I do not wish to suggest that centralised identification systems are only used by states for ill—that would be far too simplistic. Their administrative power can also be put towards nobler uses; to not only control and suppress citizens, but also to recognise and respect them (Higgs, 2004, p. 201). This is, in many ways, the primary tension of state identification systems; one that is only exacerbated by the power of computerisation, and its later digitalisation. Greater legibility can be positive or negative, and sometimes both at once. State recognition is often deeply valuable, conveying judgements of equality as well as of moral and political worth that open the door to a fuller enjoyment of liberty. Being added to the Electoral Register, for instance, underpinned democratic recognition for women and young people in the 1900s. And, as mentioned, the burgeoning welfare state that reformers like the Webbs so valued also depended on identification.

But, given the threat to liberty that centralised identity cards were linked to after the war, was going all-in on centralised welfare administration worth the risk? After all, to ensure the right people were benefitting, and had paid sufficient tax to qualify for support, the citizenry had to be made legible at a massive scale, in terms the central state could define and manage. Although National Registration and identity cards had been scrapped, the unique ID numbers people had been assigned would therefore quietly live on, embedded in National Insurance cards, NHS Numbers, and voter registration records (Higgs, 2011, p. 156). And, at Smedley Hydro—a hotel and spa in Southport, which had been requisitioned during the war[47]—these identity records

[47] My thanks to one of my interviewees, Phil Booth, for bringing this to my attention. Various records are, in fact, still held together at Smedley Hydro.

would remain centralised, despite the fact that fears about central, surveillant oversight had dominated the public debate around repealing identity cards. The site would consequently take on a quiet importance in the years to follow, as various systems based there would be administered via electromechanical tabulators, and later modern computers, with little public knowledge. Indeed, tens of millions of computer records—approximately one for each citizen of working age and above—would eventually be created to facilitate the reliable identification of almost the entire adult population of Britain. As a result, the information state underwent a truly historical transformation and, by the late 1960s, the civil service managed possibly the largest computer installation in the world[48] (Hicks, 2019, p. 23).

These new technologies brought with them novel 'technological affordances' that enabled civil servants to do new things, including new ways to discriminate (Davis, 2020). Deciding who was eligible for support, for instance, now depended to some extent on the parameters that civil servants had programmed into computer systems. By centrally recording, encoding, and tracking information about citizens' lives, Whitehall bureaucrats could in effect therefore define the bounds of acceptable identities for people around the country—without the need for physical identity cards. While this no doubt removed some of the arbitrariness of prior decentralised systems, not least by further limiting local discretion based on personal relationships and first-hand knowledge, in doing so it also increased the scope for mandarins to define 'in' and 'out' groups via the categories they programmed. As historian Mar Hicks (2019, p. 26) has shown, trans, nonbinary, and genderqueer people consequently found themselves particularly constrained by the new systems. Their records were centrally flagged as "aberrant" as a matter of policy, procedurally disadvantaging them by necessitating slower, manual reviews of their support claims (Hicks, 2019, pp. 27–28). And, as welfare pay rates were differentially linked to sex, these decisions also materially affected the levels of state support they received. Having experienced relative freedom to define their gender identities during the war years, the encoded inflexibility of centralised electronic identity records therefore amounted to explicit discrimination.

This was not the only way in which identification was used to discriminate during the postwar period. Computers, of course, had not entirely replaced older technologies. To take another example, people across the Empire had all historically shared the same status as British subjects. But the British Nationality Act 1948 had introduced the notion of common citizenship across the UK and its colonies, jettisoning subjecthood. Former colonial subjects had consequently begun moving towards the "imperial centre", exercising rights extended to them through the newly-founded Commonwealth (Torpey, 2000, p. 149). In particular, vigorous Kenyan

[48] The government even held a stake in International Computers Limited, the company supplying most of the machines, given how important they were for the centralisation project.

nationalism in 1963 had sent its "considerable Asian population into a panic" that threatened to end with the group's mass migration to the UK (Torpey, 2000, p. 150). The Secretary of State for Home Affairs had therefore attempted to render Asian Kenyans essentially stateless, despite their possession of legal British passports. The move was promptly condemned as racist by the International Commission of Jurists, and international pressure eventually forced the government to capitulate (Torpey, 2000, p. 151). But this nevertheless again showed how identification technologies were now regularly being used by the state to exclude groups from the political community. This was happening both abroad, as it had long done via the older technology of passports, to curtail freedom of association and movement of ethnic minorities, and at home, via the newer computerised welfare system, to limit state support and negate of freedom of expression for queer groups, amongst others.

3.4.3 Citizenship vs. Subjecthood

Through different identification systems, whether computerised or not, marginalised groups would thus continue to be harmed by the state. In particular, such systems allowed for an individual's legal, moral, and political status as an equal citizen to be denied. Out groups, as defined by the state, were labelled as aberrant or lesser, and so disadvantaged—computers just made administering the discrimination easier. To end this chapter, I consequently want to briefly consider the concept of citizenship, its links to identification, and reflect on just how dramatically this had all changed throughout the Industrial Age. Philosophically, of course, citizenship is usually justified via social contract theory; a rich tradition that stretches all the way back to Thomas Hobbes, John Locke and Jean-Jacques Rousseau, if not the ancient Greeks (D'Agostino *et al.*, 2024). Hobbes was particularly influential, and famously imagined life without state protection in the seventeenth century to be "solitary, poor, nasty, brutish and short" (Hobbes, 1651, p. 78). Given that he was writing in the midst of the bloody English Civil War, this is perhaps unsurprising. But the corollary of Hobbes' hypothetical 'state of nature' being so repulsive was that it more than justified, in his eyes, any loss of liberty that collective submission to a powerful monarch might entail. Along the lines we have discussed, however, this posed a problem for later classical liberals as, to avoid returning to these conditions, Hobbes countenanced the creation of an almost limitlessly-powerful state. Since, much ink has accordingly been spilled—by classical and new liberals alike—delimiting the relative power of the state versus that of its citizens.

Thankfully, though, liberals of all stripes generally agree on the basics. The gist of a social contract is that the state's legitimate power over individuals stems from the willing agreement by members of society to cooperate for social benefits (Conover, 1995). The evolution of democracy and gradual elaboration of civil liberties over the course of the Industrial Era therefore clearly adhered to this ethos. Various reforms first codified parliamentary supremacy over the monarch, then gradually expanded the franchise to working class men, and eventually women. The contract grew,

deepening the bonds and reliance between citizens, even as foreigners were excluded from the political community. This consequently reflected a shift from despotic to infrastructural power, as the state transitioned from absolutist monarchical rule to a modern liberal democracy that safeguards political rights via democratic processes and the willing consent of the people. Yet it was under Rawls's long shadow in the postwar period that the social contract approach was truly cemented as the default critical lens for the modern, liberal-democratic welfare state (Forrester, 2019). For Rawls (2005), citizens granted the state legitimacy via a *hypothetical* social contract, rather than formally agreeing, and so were assumed to have rationally given up a degree of liberty in return for state protection and the means for communal cooperation. Citizenship of a specific political society—the liberal democratic nation-state—thus fundamentally grounds this relationship.

Why, then, is citizenship of such democratic importance? Primarily, "it is through the granting of legal status as a citizen that a modern state officially recognizes someone as a member of the political community" (Carens, 2013, p. 20). If this chapter has shown us anything, however, it is that citizenship is not a given. Who counts as a citizen, or subject, has shifted constantly throughout British history[49]. It therefore pays to remember that the (hypothetical or otherwise) social contract is only a metaphor; one that can mislead us into thinking citizenship involves the willing and voluntary consent of free citizens. In actuality, as we have seen, citizenship is mostly automatic—a result of being born in the 'right' territory or by the 'right' parents, as defined by those with state power[50] (Bauböck, 2018). Although migration may thus allow a lucky few to join a different political community, this can be hugely expensive and difficult, and even then citizenship is not always guaranteed. In the postwar period, for instance, we have seen how simply residing within the nation-state's borders was no longer enough to be counted as a citizen. Instead, it was by confirming citizenship *through identity documents* that the modern state began to grant citizens legal and moral standing, and so access to rights and public goods (Lips *et al.*, 2009b, p. 835). Even then, equality was not assured—some citizens would still possess 'more' freedoms than others, as demonstrated by wartime identity cards and passports. But, by the end of the Industrial Age, we can see how far one's ability claim to an identity had come to depend upon willingness to submit to the state identification apparatus; cementing the central importance of identity systems for modern rights, liberties, and citizenship.

[49] Debates about the scope of the political community continue to vex political philosophers, c.f. Carens (2013); Kukathas (1996); Kymlicka (1996).

[50] As Higgs notes (2011, p. 79), the English poor of the pre-Modern period were not citizens as we use the word today, either. Though they did exercise some meagre rights in limited, situated, local contexts, they could not for instance vote.

3.5 Normative Conclusions

Over the twentieth century, increasingly formalised, centralised, and computerised state systems had consequently displaced a great deal of the social and local means of identification that had previously dominated in Britain (Higgs, 2009, p. 350). The political community—once effectively constrained to one's immediate, regional neighbours—had become countrywide, and this growth had necessitated new ways of proving who you were; both to your neighbours and, more importantly, to the state. In effect, the sociological narrative around identity in industrialising nations had, at last, therefore come true—albeit two centuries later in Britain than for many of her peers. Thanks to the administrative shocks of two successive World Wars, the power to define who Britons were had, at least in official contexts, finally been centralised into the hands of mandarins and their rigid systems of (predominantly) paper-based identification. Early computers then bolstered this power, enhancing administrator's means for central oversight and control with greater information-processing capabilities, empowering them to define the formal identity categories people could occupy. As the state's centralised administrative power reached its zenith in the postwar period, identification had thus been made a key aspect of everyday life. And, although citizens no longer carried identity cards, they were nonetheless recorded, managed, and surveilled through central identification databases.

One clear takeaway for my developing reflective equilibrium, then, must be that identification systems were, and still are, fundamentally tied up with the state's ability to filter, socially sort, and discriminate. On this point, surveillance state theorists would wholeheartedly agree. Whether or not you were part of the nation's 'in' or 'out' group was now almost entirely defined by formal processes and systems of identification, with the borders transformed into a site of particular restriction, observation, and coercion. Additionally, the foregoing shows how private corporations were, from the very start, essential for the development of computerised identity systems—an interesting piece of context for future chapters. This must all be kept in perspective, though. The surveillance that could occur was not remotely equivalent to that which the state can prosecute today. Early computers were not digital, and so the state bureaucracy was still essentially constrained by paper's materiality. Beyond the borders, levels of surveillance therefore waned as normalcy returned after the war. And this was very much a political choice, as other governments continued to push the boundaries of what analogue technologies made possible. The East German Stasi, for instance, had amassed detailed files, numbering approximately one billion records, on an astonishing 5.6 million citizens during the

forty years it operated after the war[51] (Curry, 2008). British governments, by contrast, allowed the wartime surveillance apparatus to be dismantled, despite the losses in their infrastructural power which resulted.

Concurrently, identity systems had also underpinned the single greatest realignment of the social contract in centuries, bringing universal healthcare and social security to millions for the first time. Reductions in state surveillance therefore did not mean that state interference was reduced—governments' promotion of positive liberty would continue. Yet it was for precisely this reason that eagerness to be registered by official systems could not just be put down to false consciousness, as some surveillance state theorists would suggest. It was, after all, by submitting to central registration and identification that people were now made citizens in the eyes of the state. This recognition was, and still is, a powerful force (Carens, 2013, p. 59). What I have called the central tension of state identification must thus also feature heavily in any eventual equilibrium; that greater legibility can be positive or negative, depending on one's relationship to those with power. Accordingly, it certainly at this point seems that modern liberals will uneasily relate to identity systems, as they can empower individuals—granting them access to rights, resources, and recognition—but only because someone first decided to lock the benefits of citizenship behind an identification system. As we go on to consider how faster, more powerful computers, joined together into networks, developed over the twentieth century, we must consequently pay close attention to the qualitative differences that digitalisation brings to the equation.

[51] To put this into perspective, the American National Security Agency was collecting approximately five billion phone records per day over half a decade ago—and capabilities will only have ballooned since (Gellman, 2023).

Chapter 5.

Centralising Digital Identity Systems in Britain

> "The ID project looked at one point as if it was a big database, Big Brother mechanism in order to provide identity authentication. […] That is not the best way of doing it."
>
> *– Richard Heaton, Permanent Secretary for Cabinet Office (2013)*

Armed with an understanding of Britain's historical identification practices, we now stand better equipped to evaluate the state's initial attempt to digitalise its existing identity systems. After several decades of relative postwar consistency, in the twenty-first century identification in Britain again entered a period of radical change. As digital computers swept through the public and private sectors—and especially became networked via the internet—they precipitated a revolution around identification practices, with new technologies enabling novel possibilities for remotely proving who people were. Yet these possibilities also brought with them significant and unprecedented normative effects. This chapter accordingly details how the British state took its first steps towards instituting a national digital identity system around the turn of the millennium, blending judgements and principles extracted from the literature with a variety of insights that arose from the qualitative interviews I conducted with a series of domain experts. As with the historical content we have already considered, throughout I emphasise the relevant changes for liberty, equality, and citizenship to highlight the changing nature of identity provision in Britain—vital context for informing the analysis of subsequent systems and policies that follows in later chapters.

Before then, this chapter argues that the shift towards digital identification—which began in earnest with New Labour's identity card scheme—was both necessary and desirable. To detail why, I first explain how the popularisation of computers had made people's lives easier while also opening them up to new fraud and inclusion risks. I also problematise how, as the central state responded to these growing issues, resurgent fears around undue centralised state surveillance and oversight once again came to dominate much of the public and academic discourse, crippling the rollout of what could have been Britain's first digital identity system. Alongside this, I evaluate the extent to which the identity card scheme should be considered a truly digital

identification system in the first place. This helps clarify what is different about digital systems, as opposed to the state's existing identification systems and methods. At the macro level, I accordingly argue that the state tried to make individuals' actions increasingly transparent to its computerised administrative systems during this period, in a troubling way, despite the ultimate failure of the identity card project. And the increased state legibility, and associated social sorting this precipitated, was only afforded to decision-makers by its central control of the relevant digital technologies. This paves the way for understanding why government was forced to step away from running the state digital identity system in the next chapter.

5.1 Beyond Traditional Identification

Introducing digital identification methods in Britain would have constituted a significant break with the past. But understanding why requires us to evaluate what, precisely, is different about digital identification—in contrast to the historical methods covered in the last chapter. As Higgs notes (2009, p. 350), the systems we have thus far considered all employed one of just two fundamental approaches to identity: the 'recommender system' alongside the increasingly favoured method of paper document cross-checking. The former technique involves trusted people vouching for others in the community. This mostly means upstanding members of society (i.e. people working in one of 'the professions') staking the identities of colleagues and friends; doctors or lawyers countersigning passport photos, for instance, to assert they are representative. For the latter, documents presented by individuals—their identity claims—can either be compared to records held centrally or else to other concurrently presented documents to spot attempts at fraud. Names and addresses on utility bills, for instance, can be cross-checked against an individual's drivers licence. False title deeds can be compared to copies held by the Land Registry. Or, more basically, signatures can be compared to those taken previously. In general, even today, Britain has not moved much past these traditional techniques—even if their administration has been made more efficient through gradual computerisation of the state's paper-based bureaucracy over the twentieth century (Margetts, 1999).

It is nonetheless essential that we understand why these two traditional identification methods began to be deemed insufficient around the millennium, making space for the articulation of new, digital approaches—not least because so many systems based upon them remain vital today. A good place to start is where many of us will have first encountered these traditional processes, at birth, when our formal identities as citizens are embryonically-established through the registration of so-called 'birther' or 'breeder' documents with the state (Nyst *et al.*, 2016, p. 28). For those not born in the country or who enter as migrants, different mandatory processes (which we will discuss later) ensure that officialdom has some idea of who resides within its borders. But, for any births on British soil, one or both parents are obliged to record their own details, along with their child's name, sex, date of birth, and place of birth, at the hospital or a local registry within 42 days (21 days in Scotland) (HMPO,

2023). One parent will sign the birth certificate, which is countersigned by the registrar, i.e. utilising the recommender system. Meanwhile, corresponding records are still collated at the General Register Office, at Smedley Hydro, so they can be cross-checked throughout an individual's life. For most individuals, birth certificate issuance therefore marks their first interaction with the information state's identity apparatus—and provides foundational evidence of their claim to being a British citizen.

Given the symbolic importance of birth certificates, I will use them as a jumping-off point to illustrate a variety of issues with Britain's traditional identification documents and methods. These are the 'binding', 'inclusion', and 'appropriateness' problems. First, however, I wish to briefly address a preliminary concern to do with the citizenship conferred by birth certificates; one that emerged during my research interviews. Identity expert Kaliya Young put it to me that birth registration—our very first state interaction "as citizens in a liberal democratic nation"—could be seen as inherently non-consensual "because our parents do it for us." I recognise that there is something ironic about this aspect of birth registration. It recalls Baubock's point that citizenship is mostly accidental and automatic, not intentional (Bauböck, 2018, p. 264). Yet I wish to make clear that I do not find this that concerning[52]. We generally accept that parental consent is sufficient for all manner of important decisions (such as vaccinations) taken on a child's behalf before they reach maturity. Why should birth registration be any different? Under modern international law and the nation-state system, lacking citizenship is a devastating fate—which is why stripping citizenship is a highly controversial practice (Webber, 2022). We should therefore wish for our children to be readily granted citizenship, whether or not they have consented to being a citizen of a particular country. The alternative is entirely undesirable, and children can always (in theory) consider emigrating later in life, should they so wish.

5.1.1 The Binding Problem

With that said, let us now explore the three central issues surrounding Britain's traditional identification methods. All are important for understanding where the assumed need for digital identification methods came from. But the first is particularly troublesome for birth registration, and illuminates one of the main drawbacks with document cross-checking. Namely, birth certificates make for very poor proofs of identity (Kent *et al.*, 2003, p. 13). This can be put down to two main reasons (Bohm & Mason, 2010, pp. 45–46). First, people often change their name throughout the course of their lives, most obviously during marriage, or otherwise do not go by their registered birth name for any number of other legitimate reasons. I, for instance,

[52] More interesting to me, is the fact the Victorians made birth registration with the state mandatory in the first place, as discussed in the last chapter. This moved us further beyond the general historical assumption of state non-interference, by necessitating some degree of centralised surveillance of the civil population—the knowledge-gathering precursor to state action.

generally go by Charlie—though my given name is Charles. Actors and authors may use a stage or pen name. And some people with foreign names will go by an adopted, local name. Yet none of these names would be reflected on birth certificates, limiting their usefulness[53]. Second, and more damning, is that a birth certificate's utility as an identity document is almost completely undermined once we realise that nothing about the document links or binds it to its original owner. As relatively basic paper documents, they are easily stolen, altered, or faked and, in reality, cross-checking with the GRO is rarely done. It therefore "does not follow that the person whose name is on the certificate is the same person as the individual in whose possession the certificate rests" (Bohm & Mason, 2010, p. 46).

Due to this binding problem, a birth certificate is not a very useful tool for proving who the person stood in front of you actually is. It does little more than record a historical event: that someone was born, and that they were given a particular name by their parent(s). Although, as a ritual process, birth registration establishes official personhood in the eyes of the state, the document itself does not have much value for identification throughout the rest of a person's life. Consequently, any public or private service providers relying on birth certificates usually have to cross-check them with a whole range of other sources of identity evidence, such as utility bills, doctors' notes, various benefits letters, and/or immigration documents. Doing so helps build a fuller picture of the person presenting a certificate; boosting the probability that they really are who they say they are by providing some corroborating evidence. Yet this kind of circumstantial cross-checking is a relatively messy solution—not least because it is an inexact art that adds significant administrative burden for service providers (Barnard, 2020, p. 19). And it is also burdensome for individuals, who must collect, store, and repeatedly present a bundle of such documents to prove who they are in different situations. Losing or forgetting to bring any one of these documents is therefore a serious inconvenience. Overall, then, identification processes built on the cross-checking of birth certificates with other documents are rather inelegant; they do not work particularly well for anyone involved.

Yet, despite these failings, birth certificates are still considered foundational identity documents. They are required to apply for, amongst other things, your first passport and (with additional evidence) first driver's licence, and can also be required as proof of age when enrolling children in schools[54]. Until recently, birth certificates were even required to get married in Britain. We are therefore faced with a conundrum. Birth certificates have been made, and remain, an important tool for proving who you are to the state bureaucracy throughout a normal life. But they are not very well suited to this task. Is there not a better solution? Thankfully, many of us

[53] Birth certificates can, however, be updated if an individual's affirmed gender changes and they can evidence this change with a Gender Recognition Certificate.

[54] Many of the alternative forms of proof for school enrolment, such as passports, in turn themselves rely on birth certificates.

will also possess other, more suitable, documents—namely, passports and driver's licenses. Not only are these more pocketable and robust than paper certificates, but they also solve the binding problem: photographs (i.e. facial biometrics) provide a simple, if not foolproof, way of checking whether the person presenting a document is its legitimate owner (SM Smyth, 2019, p. 13). And, as both are also more regularly updated than birth certificates, the likelihood that the names, addresses, and other details (like gender) will accurately reflect the person presenting them here and now remain higher, meaning these documents better lend themselves to any further cross-checking that might be required[55]. Passports and driver's licences are accordingly far more useful forms of identification than birth certificates, due largely to the fact they are bound to the individuals involved via bodily identification techniques.

5.1.2 The Inclusion Problem

Binding, however, is just the first issue. The second is that, notwithstanding the advantages passports and driver's licences have over birth certificates, many people in Britain simply do not own one. As one senior government contractor explained to me, as much as 20% of the British population—roughly thirteen million people—effectively has "no ID, like, no usable ID". Other estimates vary. The Open Identity Exchange (OIX), a former industry body for digital identity providers, pegged the number of what it calls the 'ID challenged' in the UK—those that "cannot verify their identity through traditional means as they lack the ID documents typically used"—at just under six million (OIX, 2021, p. 3). Whichever figure is correct, the fact that many millions of people in Britain cannot effectively prove their identity with one of these two documents should strike us, I suggest, as quite shocking; primarily because it poses severe inclusion-related issues. Birth certificates are, after all, required in a relatively narrow set of use cases. But passports and driver's licences have effectively become the primary form of photo ID in the country[56]—presenting them has been made necessary in all manner of situations. Just think of buying alcohol or tobacco, entering a pub, bar, or club, or collecting parcels, not to mention holidaying abroad, driving a car, or interacting with any number of services. One if not both of these two forms of identification are all-but essential for many aspects of everyday life in contemporary Britain, particularly for younger citizens, regular travellers, and drivers.

Given the importance and utility of these documents, though, why do millions of people not own them? Alongside religious or cultural reasons and a general mistrust of government, a primary reason for many is the cost of acquiring and updating these documents (Coles-Kemp & Heath, 2020, p. 4). Indeed, in line with what we might

[55] Passports (though not driver's licences) also include microchip-based security features that can help check for tampering with the printed information on the document.

[56] Schemes like PASS present an alternative, allowing (primarily younger) people to buy proof of age photo cards, which can also help fill the gap, but are nowhere near as ubiquitous as the main forms of photo ID.

expect if this were true, we see that populations in receipt of government financial support often struggle the most to identify themselves. Cheryl Stevens, Director of Shared Channels Experience at the DWP, told me that her department repeatedly came up against the fact that "people didn't have passports or driving licenses", and neither could her teams "rely on credit reference agencies, because I know that they are three of the big key things that our customers can't pass". Running a car, travelling internationally, and maintaining good credit are relative luxuries for anyone struggling to make ends meet. And all these identity documents—birth certificates, passports, and driver's licences—are costly to acquire and update. Birth registration itself is free, but acquiring a certificate currently costs £11 per copy. Passports cost between £82.50 to £104 for adults, depending on whether you apply online or by post. And your first driving licence will currently cost either £34 and £43, again depending on how you apply. For those already having to make tough choices about how to spend limited income, acquiring such documents can consequently seem like non-urgent considerations.

Relying on the traditional forms of identity evidence therefore raises distributional issues around inclusion and equity. And, again, the effects are likely to be felt most by already-marginalised groups. Take, for instance, the Home Office's *Right to Work* and *Right to Rent* schemes. Introduced in 2016 as an extension of the already decade-old 'hostile environment' policies, these schemes aim to make life difficult for undocumented migrants in the UK (W Williams *et al.*, 2020, p. 65). They require anyone attempting to formally secure housing or a job to present passports, birth certificates[57], or immigration documents (including digital 'share codes' created for this purpose) to the company or landlord they are dealing with. Many people, especially in the British middle classes, will consequently have little trouble proving their identity for these purposes. By contrast, many of the groups identified by OIX as ID-challenged—immigrants, but also the young, poor, urban families, elderly people, and those living in 'rural solitude'—will not fare so well (OIX, 2021, p. 11). In effect, identification has therefore been made an additional burden for some in society who are already most in need of housing or a job. And OIX highlighted how these groups' struggles with identity will not end there. A further corollary of not being able to afford sufficient identification is that these same groups' identities are more easily stolen. Such groups, as fraud expert David Black explained to me, are thus effectively doubly-disadvantaged, as the sky-high costs of fraud and identity repair fall hardest on those who are already struggling to prove their identities.

[57] If providing birth, adoption, or naturalisation certificates, these must be corroborated with other forms of evidence, such as official letters from a previous employer or government agency. For Right to Rent, but not Right to Work, the recommender system can actually still be used—a letter from someone in the 'accepted professions' can be accepted in conjunction with various other forms of proof.

We should also note here how migrants are, as usual, particularly disadvantaged by the British state's inadequate identity infrastructures, somewhat cruelly and performatively. As philosopher Joseph Carens (2013, p. 63) has argued, it "is certainly possible for [migrants] to be citizens, to have equal legal rights, and to be marginalized nevertheless". Forcing people to regularly disclose that they are migrants, via identification processes, is one way in which the state can remind people of their 'othered' status. And we have already seen how there is a long history of such discrimination in the UK. More recently, the infamous Windrush Scandal has been especially illustrative. For many of the Commonwealth citizens invited to settle in Britain between the 1950s and 70s, a lack of official identification—which the state failed to provide, despite migrants' legitimate claims to citizenship—has been used to systematically persecute those of Caribbean origin (Webber, 2022). As the independent review makes clear, the Windrush generation were "treated appallingly" (W Williams *et al.*, 2020, p. 113): "Some were removed from the UK, some spent time in detention, some lost jobs, homes, healthcare and precious time with their families. Many lost their very sense of identity." And research found that Right to Rent contributed by increasing "discrimination by prospective landlords towards both BAME people and foreign nationals" (W Williams *et al.*, 2020, p. 109). In the twenty-first century, centralised identification tools have thus retained their status as the British state's tool of choice for defining 'in' and 'out' groups—vital for excluding and suppressing the liberties of those seen as 'lesser' by those in power.

5.1.3 The Appropriateness Problem

This brings us to our final concern with traditional forms of identification in the Britain—and potentially the most puzzling. This is that birth certificates are actually the only formal proof of identity we have so far discussed. Unlike many of our European neighbours, British citizens face no legal requirement to carry identity documents, so the state simply does not issue them (Fishenden, 2020, p. 5). You will never be stopped in Britain and asked to present 'identity papers, please!' by the police[58] (Rolph, 2004); indeed, such requests would traditionally have been considered an affront to 'Britishness' (Agar, 2001). While passports and driver's licences may therefore be regularly used for identification purposes, neither are technically identity documents. They are, in fact, nothing more than 'optional' extras that some citizens choose to acquire but no citizen would ever be legally expected to possess outside of their intended function. Passports are, of course, travel documents; permissions to cross a border, and a reminder to foreign nations that Britain's citizens are under the protection of her government. Driver's licences, too, are merely another proof of entitlement; permissions to drive. And these distinctions are vital. As identity expert Adam Cooper put it to me, although both are used as "de facto identity" documents,

[58] Though you may be asked to present yourself at a police station within seven days to confirm your identity, giving you time to collect various forms of identity proof.

they are in fact better thought of as "part of the proof of your identity". Passports and driver's licences can certainly help verify an identity during a cross-checking process, much like any number of other pieces of evidence, but are not themselves identity documents[59].

Today, the departments responsible, HMPO and DVLA, accordingly find it frustrating that their documents have become so ubiquitously used as identity documents. Neither was developed with this intent, and nor does formal identification sit within either departments' policy remit. As one senior civil servant working on identity policy put it to me, there is thus a disconnect between "the official policy stance and the reality of how people use both passports and drivers licenses"—between what the DVLA and HMPO will accept, and how their documents function in reality. This disconnect is the source of numerous issues related to British identity practice and, in turn, is indicative of the gap between what we have and what we need when it comes identity policy in Britain. In effect, parts of the administrative state operate as if citizens have a universally effective form of identification, even if in reality millions do not. And, as OIX's Nick Mothershaw pointed out to me, it is only where stop-gap documents have explicitly "been written into particular regulations, like those around anti-money laundering" that they are even legally acceptable as forms of identification (i.e. 'you can accept a passport/driving license as proof of ID'). The net effect is that this is an interesting case of scope creep, wherein these documents have inadvertently come to fulfil a genuine need in society for more reliable forms of identification which the state has not addressed.

The peculiarity of this situation is not just of academic interest, either. As one senior government contractor reminded me, because these documents were designed for a specific purpose, both can also be removed by the state without concern for the knock-on inclusion effects—deteriorating eyesight might leave the elderly without driving licences, for instance, or a football fan's passport can be confiscated to prevent sports-related violence—deepening the existing inclusion issues we have identified. Policymakers have therefore constructed a situation in which there are limited identification-related rights for British citizens. As the state does not issue us with formal identity documents, citizens cannot stake claims to such goods, or seek much redress if their documents removed—even though the state has made enjoying the fruits of citizenship increasingly dependent upon presenting identity documents in the first place (Lips *et al.*, 2009b, p. 835). Arguably, this was intentional. Again, the Windrush Scandal is instructive here, as the official report found the British state "firmly placed the onus on the person exercising their rights, rather than the Home Office, to prove their status" as a citizen (W Williams *et al.*, 2020, p. 56). Decades after the Windrush Generation first moved to the UK, tens of thousands of British citizens

[59] A huge number of my interviewees impressed this distinction upon me, as it is a common misconception amongst non-experts.

were thus illegitimately deported due to their lack of identification, while the state "progressively eroded the rights" of those that remained (W Williams *et al.*, 2020, p. 118). And similar effects will continue to be felt by many other people in Britain who, for various reasons, cannot sufficiently prove their identities.

5.1.4 Towards New Identification Methods?

So, there are a number of issues relating to traditional identification documents and methods in Britain. First, the documents many use most often to 'prove' their identities in everyday life, passports and driver's licences, are not identification documents at all. More concerningly, many millions of Britons also do not even possess these documents in the first place, making it harder for them to access various private and public services. Third, the closest thing we have to a formal identity document, the birth certificate, is not remotely fit for purpose either. It provides no assurances that the person presenting it is the person to whom it rightfully belongs and, as you will recall, was primarily developed by the Victorians to aid in the collection of civil statistics, not support day-to-day identification practices. Finally, all three of these documents are fundamentally underpinned by decidedly-analogue identification methods that have seen little meaningful change in centuries—despite attempts to bring passports and driver's licences into the twenty-first century[60]. A modern, purpose-built digital identification system could therefore be a possible solution to all of these issues. But what would a digital alternative look like? How would new, digital identification methods differ from the recommender system and document cross-checking processes that have served us well for centuries? Unpacking these questions will require us to consider the role of the internet—and the impetus it provided for the development of new identification methods around the turn of the century.

5.2 Identity on the Internet

Like many modern technologies, digital identity systems owe a great deal to the internet. Not discounting the importance of the traditional systems we have already evaluated, the internet's history is intimately bound up with that of modern identity systems; and is vital for understanding our current situation. But we must also be careful not to read back into the past. In the wake of the Snowden Revelations and Cambridge Analytica scandal, dystopic undertones have characterised much recent scholarship around the internet. Yet, in the early days, the prognosis was far more optimistic. Psychologists, social scientists, and philosophers wrote extensively about

[60] Passports have perhaps seen the most evolution toward this goal. But their digitalisation has mostly taken a supplementary form, rather than reforming the document as whole (I discuss this further below). Passports are, after all, a documentary proof that are still manually checked and stamped at many passport control desks around the world, despite the addition of biometric chips and computerised databases to improve their effectiveness.

the internet's revolutionary potential around the turn of the century, particularly for personal identity performances (rather than identification per se). Sherry Turkle's (1995) foundational study typifies the sense of freedom and opportunity around identity that accompanied widespread internet adoption in the mid-1990s. Newfound online "anonymity", she argued, had given "people the chance to express multiple and often unexplored aspects of the self, to play with their identity and to try out new ones" (Turkle, 1995, p. 12). The internet was accordingly a place where people could endlessly reinvent themselves, presenting different aspects of their personal identities across multiple contexts—a resurgence of the Goffmanian utopia where, freed from the limits of physical embodiment and formal documentation, people could be whoever they wanted to be (boyd, 2007, p. 129).

This optimism around identity fit well with, and indeed was magnified by, the libertarian leanings of early internet pioneers, who explicitly saw the internet as a "technology of freedom" (Pool, 1983). 'Cyberspace', they thought, could be a world beyond central governmental control and oversight, giving citizens a way to reclaim (at least virtually) the liberties that states had wrested from their populations (Goldsmith & Wu, 2006). This extended to a rejection of the need for state-backed identification. Legal names were not required—by law or custom—to post on most early websites, and so many interactions were at least pseudonymous, if not outright anonymous. For the small communities of academics and military researchers that compromised most of the earliest internet users before its widespread adoption, this did not present a big problem. Other people could, implicitly, be trusted or vouched for by mutual contacts, and the transactional stakes were relatively low. What little identification taking place, then, was reputation-based (i.e. utilising the recommender system) and so essentially social in nature (Lehdonvirta, 2022, p. 42)—much like in the classic sociological story around pre-Modern identity in industrialising societies that we discussed in the previous chapter. There was no need for recourse to formal, state identification; community knowledge was generally sufficient, and safe participation on the internet did not particularly rely on knowing the legal identities of the individuals you were communicating with, given the many mutual ties amongst this small community.

As the internet matured, however, more business and governmental transactions gradually moved online, accompanied by millions of new users. The pivotal moment came in autumn 1993, the 'September that never ended', where the usual trickle of new users became an overwhelming stream (Grossman, 1997). This strained the libertarian ethos of the early web. Particularly in emerging high-stakes situations, like online banking or e-commerce, a new 'identity problem' started to grow, as individuals and institutions found they needed ways to remotely "ascertain identities" of the digital masses to ensure they were dealing with the right people (Chango, 2012, p. 10). To illustrate with just one example: economist Vili Lehdonvirta (2022, p. 47) has shown how social norms and reputations became insufficient for securing the early large scale online marketplaces, and so made managing the risks involved in

exchanges of any real value extremely difficult[61]. Just as sociologists had suggested in the context of industrialised cities, the socially-rooted approach to identity was therefore again failing in the face of massive population growth. Over a few short years, the internet consequently retrod decades of offline human development. Identity performances would remain an important aspect of internet culture, but solving the internet's emerging identity problem would require developing robust means for achieving the formal identification of individuals online (Kerr *et al.*, 2009, p. xxiv). It would, in other words, require the development of digital identity systems.

5.2.1 Early Work on Remote Authentication

Initial work on digital identity infrastructures was driven by commercially-oriented technologists building complex, cryptographic systems for corporations (Eaton, 1999). I will avoid technical detail wherever possible in this chapter, and those to come, though functional overviews of certain technologies will of course be necessary to contextualise our discussion of their moral and political impacts[62]. This will not begin with identification, however, but with the closely-related process of authentication. In Britain, the first hints of change around authentication practices actually surfaced a few decades before internet use took-off, in the 1960s. According to Higgs (2009, pp. 190–191), the primary catalyst was the rollout of automated banking, followed much later by internet banking, against a backdrop of tax centralisation and public sector computerisation[63]. Throughout this period, regular, remote interactions with public and private service providers became increasingly normal for much of the British population. But allowing customers to remotely access high-value services via ATMs, phones, or the internet required the creation of new secure access solutions. As bank clerks, for instance, would no longer necessarily know the customers they were dealing with—let alone be able to check their documents when interacting face-to-face—novel approaches to keeping customers'

[61] On sites like eBay, the laid-back approach to identification caused particular issues. The founder and site administrator, Pierre Omidyar, could not adjudicate every complaint made against fraudulent or dishonest buyers and sellers, and indeed due to his libertarian sympathies did not want to assume such authority (Lehdonvirta, 2022, p. 39). His solution was thus to develop a community reputation system.

[62] Most modern identity architectures are built on the relatively ancient (in computing terms) Public Key Infrastructure (PKI) technology (Windley, 2005). Digitally signed cryptographic keys, administered by certificate authorities, are distributed and used to ensure that individuals claiming to hold certain credentials are indeed their correct owners (Meints & Gasson, 2009, p. 154). Along with electronic signatures and authentication techniques like biometrics—such as fingerprinting, photographs or facial scans—PKI constitutes a key part of most digital ID documents (Meints & Gasson, 2009, p. 176).

[63] Taxation was centralised with the Income Tax Management Act of 1964 (Higgs, 2001, p. 190). This was accompanied a few years later by the creation of the Police National Computer and the centralisation of drivers' licensing in the precursor to the modern DVLA (Higgs, 2001, p. 191).

safe were needed. These had to be able to function at distance, often automatically, without relying on organisations' traditional security safeguards.

With the digital identity industry nascent, remotely identifying new customers was not an option. Customers would still need to come into a branch and provide adequate identification to setup an account in the first place. But the technology was sufficiently developed for customers to be remotely authenticated after this point, allowing them to access existing accounts at a distance using secrets, keys, passwords, and personal identification numbers (PINs), rather than physical signing receipts, cheques and permission slips (Higgs, 2009, p. 191). All of these authentication tokens essentially work in the same way. Take, for instance, computer passwords, which MIT researcher Fernando Corbató had developed back in 1961 to address his frustrations with early mainframe computers. Passwords functioned like a digital lock, and allowed Corbató and his colleagues to negotiate time-shared access to MIT's mainframe by compartmentalising research data. Without the correct password, a person's data would remain inaccessible—allowing multiple researchers to use the same mainframe while keeping their files private. The solution's wider utility was immediately obvious. Passwords therefore quickly propagated throughout the computing community and beyond, trickling down into areas like banking (in the form of PINs) within a decade[64]. So long as an account owner kept their PIN to themselves, the technology would allow them secure account access, all around the country, without the need to talk to a bank teller. The future, in the form of remote authentication, was here.

Authentication, however, is not identification. An authentication process cannot tell the bank who I am if they do not already know me. PINs and passwords do not prove identity—indeed, they were not designed with identification in mind. Technically-speaking, as digital identity expert John Erik Setsaas impressed upon me, passwords have historically granted someone physical access to an area, "like a city of fort". Even if nowadays we talk about authentication rather than access in digital systems, the concept remains the same. Anyone with the correct password is granted access, whether or not they should be, as they are merely proving they possess the right authenticator; not a specific identity. An enemy spy might compromise the password, or an individual might share their banking details with their spouse. Problems can consequently arise whenever people conflate authentication with identification. "You think you're giving them access to something," as John Erik puts it, "but in reality you're telling them, 'you can be me now'". This was an issue Corbató himself faced. By 1962, just a year after inventing the computer password, managing MIT's mainframe had become "kind of a nightmare"—password theft was rampant,

[64] Barclays' first ATM, for instance, opened in 1967. Card PINs could be repeatedly presented and compared to those previously recorded, indicating that the person entering their PIN at the ATM was likely to be the same person that had opened the account.

as researchers had realised they could steal computing time by logging into other accounts (Yadron, 2014). Although convenient, remote authentication technologies therefore also opened up new avenues for networked, identity-related fraud.

5.2.2 Password Proliferation

This problem was not, as one might imagine, confined to MIT. By the time the twentieth century drew to a close, growing rates of identity fraud linked to remote authentication were also seen by the British government as a spiralling—and increasingly costly—issue (LSE, 2005, p. 103). Organisations across both the public and private sectors were enthusiastically adopting computerised networking technologies (Margetts, 1999). But, as computers rose in popularity, the gradual "proliferation" of passwords, PINs, and secrets became almost inescapable, with all those secrets increasingly hard to keep track of (Wills, 2008, p. 175). This was only exacerbated by the poor user experiences users often faced when remotely authenticating. To reduce the risks of password theft or re-use, for instance, regular password changes and arcane rules around password choice were (and often still are) mandated by system administrators[65]—much to their users' frustration (Yadron, 2014). Yet this triggered a vicious cycle. Forced to regularly update all their different authenticators, many users began to choose weaker and weaker secrets to make remembering them easier, which in turn made protections easier to bypass for fraudsters (Eaton, 1999, p. 185). Even today, passwords such as 'password' and PINs like '123456' accordingly remain amongst some of the most popular, making compromising the associated accounts trivial (Saltzman, 2022). Rates of identity fraud would thus keep growing, cementing the issue on the national agenda.

As remote authentication technology bedded-in, some of these issues would of course be addressed through better service design, standards-setting, and user education, including the development of federated identity systems—a solution which we will consider in the next chapter. But, before then, booming identity fraud around the turn of the century increasingly led policymakers to the conclusion that government itself may need to play a central role in digitally securing identities (CJ Bennett & Lyon, 2008, p. 10). This had the potential to kill two birds with one stone: to not only show that the state was responding to the impending fraud crisis, but to also help address some of the main problems with existing forms of identification that we covered at the outset—binding, inclusion, and appropriateness. Beyond this, parts of government further realised that digitally identifying individuals to a government-backed 'gold standard' could even set the state on a path towards revolutionising its inherited backend processes—which currently were still almost all paper-based (Home Office, 2006). Doing so, parts of government hoped, might help catapult the

[65] Readers may remember products such as RSA's SecurID fobs, which were commonly deployed as addition authentication factors (using time-based one-time passwords) to provide extra security.

country and the economy into the twenty-first century, with the added bonus of positioning government as the "sole source of 'identity assurance' to the private sector" (Wills, 2008, p. 175). The impetus for developing a national digital identity system thus slotted into place, paving the way for a new state identification apparatus to be championed by an ambitious, technology-focused government.

5.3 New Labour's Identity Cards

Notwithstanding the potential benefits of such a system, the challenge the state faced was massive. Over the twentieth century, successive British governments had repeatedly failed to popularise a centralised, unified, nation-scale identification system that might function across the various contexts in which the state encountered citizens and residents. Ever since the early-1950s—when, as we have seen, wartime identification cards were again repealed, due to their perceived threat to civil liberties (Rolph, 2004)—a patchwork of variously-integrated analogue and computerised systems had instead sufficed for welfare and tax administration, as well as other organisational and managerial functions of the state (Thompson, 2008, p. 157). This had grown out of, and gradually diverged from, the remnants of centralised wartime National Registration programme. Distinct and usually direct relationships with individual departments had therefore emerged as the primary way in which people would interact with the state—entailing the needless duplication of identification processes (Lips *et al.*, 2009a, p. 721). As a result, still today most British citizens hold multiple functionally-redundant fragments of identity that are distributed, or rather siloed, across different parts of government. Examples include the NHS Number, National Insurance Number (NINO), Government Gateway ID, Universal Credit Account, Unique Taxpayer Reference, as well as passports and drivers' licences—yet many more exist beyond these.

In lieu of a central solution, these numbers allow public servants to track individuals in administrative databases. Unique identifiers, in particular, help address issues of indeterminacy; more reliably picking out an individual than their name, age, and place of birth might[66]. And our association with such identifiers starts young. Indeed, as soon as a parent applies for Child Benefit[67], the GRO liaises with the Department for Work and Pensions (DWP) to issue the child with a NINO. As an ex-civil servant pointed out to me, this is not commonly understood—individuals are only made aware of their NINO at sixteen, wherein they may formally enter work and

[66] I was probably not the only Charles Smith born on the 7th of September 1995. Even if I was, what if I was registered as a Charlie or C.H. Smith, not Charles? Or what if a transposition error was made during enrolment and the name on my presented document does not match the name in the system? Unique, alpha-numeric identifiers help solve these issues.

[67] Child Benefit is a monthly support payment provided by the state for anyone with parental caring responsibilities. A version of the payment has existed since the end of the Second World War.

the tax system. Nevertheless, claiming Child Benefit enumerates most[68] children with a unique identifier that follows them from birth into adulthood and, eventually, to their state pensions and death. NINOs are not, however, particularly reliable for identification purposes. There are many duplicates, coverage of the population is spotty, and they also suffer from the binding problem (Crosby, 2008, p. 21). Many other departments will therefore generate similar numbers for individuals themselves, rather than relying on NINOs. Since the early 2000s, for instance, almost all children have also been furnished with a Unique Learner Number (ULN) from the Department for Education (DfE). This tracks them from the age of two, through to further education and university—whether state-educated or not. Hence, the British state has ended up with a multitude of these entries for people across different contexts.

Despite this byzantine proliferation of identifiers, suggestions to follow many of our European neighbours in adopting a centralised, digital approach—where each citizen is assigned a 'master' record in a single, authoritative database—have repeatedly been met with strong civic and parliamentary opposition. As we have seen, Britons are generally suspicious of monolithic and interventionist identity practices (CJ Bennett & Lyon, 2008, p. 13). And, throughout the 1980s and 90s, Thatcherism had demonised the public sector and its perceived paternalism (Palumbo, 2004). Investment in a large-scale governmental identity programme would therefore have been a risky proposition. Nonetheless, a centralised, digital system would theoretically allow citizens to reliably and consistently prove who they are across different departments, improving their experience of public services while reducing fraud and administrative costs (Barnard, 2020, p. 17)—an appealing proposition for any government. And successful examples of such systems were close at hand in the early 2000s. Belgium, for instance, had recently replaced its "existing paper-based identity card system with a smartcard-based system that incorporates digital certificates" (Fishenden, 2005). Yet implementing a similar system in the UK ultimately proved to be problematic. New Labour's identity cards, the state's first attempt at a national digital identity scheme, were a complete political failure—to such an extent that the threat of mandatory identity cards still haunts policymakers today. Evaluating this programme will consequently allow us to uncover the characteristically normative issues that have underpinned much of this resistance.

[68] I specify most children because, as Benjamin Welby highlighted to me, the Conservative-Liberal Democrat Coalition introduced a Child Benefit exemption for high earners (the cut-off is currently placed £50,000). These children are consequently not captured in the National Insurance database until much later in life, when they begin work. Now, I am not aware of any material differences in treatment by the state that emerge from this discrepancy, but the lack of universality in the policy is interesting regardless.

5.3.1 Entitlement Cards

As Higgs (2004, p. 188) notes, though the British state had historically collected only "modest amounts of information on its citizens" outside of wartime, proposals for a voluntary, centralised national identification system were again being seriously considered by Home Office officials as early as 1989 (2004, p. 184). It is also worth noting that government data sharing, made easier by computerisation, had expanded behind the scenes since the 1980s (Higgs, 2011, pp. 188–189). This had, however, involved a lot of manual work due to the fact that a) no universal number tied an individual's records together across different systems[69], and b) the government was still essentially paper-based, despite its enthusiastic adoption of computers during the past few decades. These inefficiencies had therefore galvanised support across party lines for reforming Britain's decentralised state bureaucracy via the use of new, digital information processing technologies, coupled with the reintroduction of identity cards. John Major noted his support in 1994 for such a scheme, on the grounds it would have allowed his Conservative government to rationalise numerous databases and more easily identify welfare recipients and taxpayers (Higgs, 2004, p. 185). And, as Tony Blair's New Labour later saw it, his government's key goal of instituting "joined-up government […] went hand in hand" with identity card adoption (CJ Bennett & Lyon, 2008, p. 15). Yet these proposals did not develop past the early stages of policy design until New Labour's second term in office.

What really catalysed calls for a national digital identity system were the 2001 terror attacks in America. Biometric identity cards—initially referred to as 'entitlement cards'—were championed by New Labour during the heightened securitisation that swept through Western politics after 9/11 (Wills, 2008, p. 164). The initial framing around entitlement was interesting for several reasons. First, it pointed to the fact that identity fraud was high on the national agenda; the Home Secretary at the time, David Blunkett, explicitly tied the scheme to potential welfare fraud savings of £1.3 billion in its initial consultation (Home Office, 2002). Blunkett's argument was that identity cards would offer more reliable and secure identification than traditional documents. They would, in other words, explicitly address the binding and appropriateness problems, as Britain's first dedicated proof of identification since the World Wars. But the notion of entitlement also deepened the link that was being forged by government between being able to present a formal identity and enjoying the fruits of citizenship; cards were positioned as a way to both secure the borders and establish rightful claims to the country's resources (Lyon, 2009, p. 40). Throughout the consultation document, the Home Office consequently suggested identity cards could help deter illegal immigration by keeping irregular immigrants out of the welfare

[69] NINOs were often used as a starting point, but are not reliable enough to be considered true unique identifiers (Crosby, 2008, p. 21).

system and formal employment[70] (Home Office, 2002). Indeed, the fact that the rollout eventually began with foreigners, not citizens, provides further reason to think this was a guiding purpose of the scheme (Collings, 2008, p. 65).

At a time when 'them' and 'us' framings around the Middle East were running rampant, constructing 'true' citizen entitlement to state support thus reasserted the essentially discriminatory aspect of identification systems that we have previously covered. Such discrimination may be legal, even moral, depending on one's view of justice, but it is key to understanding part of the cards' purpose. Nevertheless, from the outset, New Labour signalled its intent to double-down on the inclusion and social sorting issues that existing non-digital schemes were already propagating. In fact, New Labour's time in office saw debates around terrorists, asylum seekers, and net migration generally take up greater space on the national agenda (David Barnard-Wills, 2012, p. 138). And digital systems, like e-borders and identity cards, were consistently positioned as the characteristically "technological fix" to an increasingly globalised and insecure world (Rhodes, 2000, p. 162)—rather than an exacerbating cause[71]. As the Home Office (2006) argued at the time, "[b]etter ways of identifying people will help us to facilitate travel for those we want to welcome to the UK. They will also help us to remove those not entitled to be here." Migrants and visitors alike were therefore newly "constructed as needing 'identity' to function in society", where identity was understood in narrowly administrative terms (David Barnard-Wills, 2012, p. 138). Again, the state was insisting that individuals would need documentary proof of identity to secure their entitlement to citizenship, when such proofs had never before been needed in peacetime. It was, in other words, once again trying to socially sort the population.

5.3.2 The Third Coming of Identity Cards

Thanks to pressure from the LSE's influential Identity Project, officials were eventually forced to more honestly rebadge the proposals as 'identity' rather than 'entitlement' cards (LSE, 2005). Nonetheless, progress on the project continued and, in March 2006, the government passed the Identity Cards Act, which made provisions for the creation of two interlinked systems (Sullivan, 2007, p. 238). Plastic identity cards (as well as new driver's licences and passports) would hold each person's personal details, including their name, date of birth, address, gender, and nationality,

[70] It would therefore also have necessitated new expectations around the regular checking of cards during interactions with both the state and business—a far cry from, say, the NHS's traditional principle of 'free at the point of use'.

[71] As one New Labour minister later put it: "I don't believe that you can avoid a Windrush situation without a data identity management system. And I don't believe you can have an effective identity management system without correlation of identity across government departments" (W Williams *et al.*, 2020, p. 63). Paradoxically, although it was due to documentary identity issues that the Windrush Generation had been denied their legitimate claims to citizenship in the first place, the answer had to be more identification, not less.

along with various forms of biometric data (Lyon, 2009, p. 40). The full extent of these biometrics was never made completely clear, but cards could have included signatures, photographs, fingerprints, and even iris scans (Aaron K Martin & Whitley, 2013, p. 56)—an extensive list, given the mistrust of bodily identification that had permeated British culture for centuries. Cards were also intended to cost only £30—half the cost of passports at the time—while being Britain's first purpose-built identity document (BBC, 2009). We can therefore grant that they would, to some extent, have addressed the inclusion and appropriateness existing solutions faced. But the most genuinely novel aspect of the scheme was less tangible. Beneath the cards would sit a massive, centralised database, called the National Identity Register[72] (NIR). This would store all the data held on cards along with additional information about cardholders—i.e. almost the entire adult population in the UK over the age of 16 (roughly 40-50 million people at the time)—and interface with various other governmental databases to support 'joined-up' government (E Whitley *et al.*, 2014, p. 207).

Although the prospect of carrying physical cards consequently caught the most public attention, the real innovation was the system's digital backend. The NIR was intended to replace a whole range of ageing, paper-based processes by equipping each citizen, whether they understood it or not, with a monolithic digital identity built atop a persistent, unique identifier (E Whitley *et al.*, 2014, p. 207). Centralisation was thus to be reasserted, once again, through identity cards, which would have reclaimed their position as the lynchpin of the entire information state. And, by taking advantage of new technologies, the scheme could have provided the means to modernise the state bureaucracy, beyond just digitising existing paper records. The addition of biometrics, in particular, was an explicit attempt to "secure or fix identity" and so solve the binding problems prior schemes had faced (Aaron K Martin & Whitley, 2013, p. 57). Relying on bodily features that could be consistently and objectively measured would, after all, have allowed the state to more reliably enrol, identify, and verify the citizens it was managing, at least in theory (E Whitley *et al.*, 2014, p. 207). Thanks to the NIR being a digital, networked database, cards would also have been newly demanded in a wide range of governmental and private sector contexts—including "opening a bank account, obtaining welfare benefits or checking the status of job applicants" (Birch, 2008, p. 190). Yet, most revolutionarily, cards were intended to eventually be made "compulsory" (Santo, 2016, p. 7). Mandatory identification, backed for the first time by digital means, would consequently have become ubiquitous once more in Britain, for the first time since World War Two.

[72] Over time, the database's structure evolved, with proposals for some of the data to live in separate (yet still centralised, even if not unified) databases (Aaron K Martin & Whitley, 2013, p. 56).

5.3.3 A Paradigm Shift?

The question therefore naturally arises: to what extent would the scheme have constituted a true break with the past? A useful way to think about this is to imagine technological development around identity systems proceeding along two different paths. Mawaki Chango (2022) has suggested this disjunction belies two fundamentally opposed philosophies around digitalisation. On the first, more "linear", path, we would remain within the familiar, paper-based paradigm of physical credentials, augmenting these older methods with digital technologies to "increase security and trustworthiness" (Chango, 2022, p. 6). Think of adding cryptographic chips to passports to prove they are genuine, or sharing digitised versions of driver's licences. This path still represents progress, but of a more evolutionary rather than revolutionary nature. The second path, by contrast, jettisons the paper-based paradigm completely. This involves fully embracing truly digital ways of working, along with all the associated affordances. Rather than transmitting digitised versions of our physical credentials over the internet, we would shift "to digitally doing digital stuff […] in the form of a fully digital (online) credential" (Chango, 2022, p. 6). This path is harder to realise as a result. It requires superseding the traditional identification methods of personal recommendation and document cross-checking with digital ways of assuring trustworthiness in an individual's identity—and would accordingly upend centuries of continuity with these methods, even if they will never fully be replaced.

By these lights, however, New Labour's scheme sat firmly in the former camp. This is not down to the physical cards, which can form part of a properly digital system. Rather, the reforms as actually realised were piecemeal at best, and the scheme still relied upon the traditional methods of identification that had predominated for centuries (E Whitley *et al.*, 2014, p. 207). Behind the scenes, databases could certainly have been connected up via each citizen's unique identifier[73], but the roll-out did not involve a thoroughgoing digital reimagination of the way government made people legible. As David Rennie, an identity expert working in government at the time explained to me, enrolment would still have required an individual to provide a birth certificate along with other corroborating evidence to an agent of the

[73] This would not, on its own, have solved the identity-related problems with physical documents and their cross-checking. As identity consultant Stephen Wilson put it to me, "identifiers are not identities". Identifiers are instead best thought of as pointers into databases, which in Stephen's words, "we should not anthropomorphise". In an age of computer-assistance filing, they would certainly make cross-checking easier. But they do not negate the need for cross-checking if there is to be any certainty around an individual's identity. So, despite the administrative advances offered by unique identifiers, the NIR would still essentially have relied on cross-checking documents presented by individuals at registration to ensure that people were who they said they were.

state, in person, to verify their claimed identity[74]. And, as budgets ballooned, plans for the centralised NIR were also watered-down, with "biographic, biometric and administrative information data" to be split up and stored "on different (logical) databases"—including some that already existed—to reuse existing data and infrastructure (E Whitley *et al.*, 2014, p. 208). The result consequently cannot be described as a paradigm shift. Adding biometrics and digitising personal data would certainly have made verification and authentication easier, while providing valuable fraud reduction mechanisms. But government would not have embraced fully-digital ways of registering, proving, and reusing identities. At most, it would arguably have only laid the foundations for a digital state—later governments would still have had their work cut-out to properly digitise identity atop these foundations.

5.4 Problems with Identity Cards

The scheme, however, would never make it that far. By the time the first few thousand cards had been printed in late 2008, a coalition of academics, journalists, and campaigners had raised considerable doubts about its viability. Financial and practical concerns were especially salient, though are less relevant for our purposes (LSE, 2005; EA Whitley & Hosein, 2010). More pertinently, the recognisably high-modernist scheme promised to significantly increase individual legibility in the eyes of the state. As you will recall, Scott (1998, p. 219) boiled high-modernism down to "standardization, central control, and synoptic legibility to the centre". And all three of these aspects were reflected in New Labour's plans. In terms of standardisation, the combination of identity cards and the NIR would have normalised the registration, documentation, and classification of the entire population. Much like with prior identification schemes, the categories set out by lawmakers and civil servants would thus have defined and constrained the bounds of the formal identities people could inhabit (Lips *et al.*, 2009a, p. 722). Second, when it came to central control, we have seen how people's rights and entitlement to state support were already being made conditional on non-digital proofs of identification, and now additionally on the compulsory presentation of valid cards. Finally, on synoptic legibility, anyone with access to the NIR could, as we will see, have enjoyed a bird's eye view of the entire population's identity-related interactions (E Whitley *et al.*, 2014, p. 207). The programme would accordingly have amounted to one of the most nakedly high-modernist political projects in living British history.

Naturally, many wondered why government needed such levels of insight into what people were doing. According to Blair and Blunkett, greater legibility would help improve public services (Rhodes, 2000, p. 151); data-gathering to boost

[74] Whitley, Martin, and Hosein (2014, p. 207) concur: the "arduous registration processes" would have involved "physical interaction with each resident […] to check people's 'biographical footprint' during the enrolment".

transparency had been promoted for decades as a way to bolster public-sector efficiency (Hood & Heald, 2006). With more and better-quality data flowing into (and out of[75]) a 'joined-up' government, the argument went, policymakers would "make smarter decisions and behave better" (Flyverbom, 2019, p. 13). Centralising digital information in the NIR was thus required because computerised information systems were "now central to the tools of government" (Margetts, 1999, p. 25). Accordingly, personal data was being constructed as a kind of novel resource or raw material for better government—a distinct argument from those that focused on entitlement and social sorting. Indeed, one government report identified a "clear virtuous circle" between identity systems and social improvement, claiming that "[t]he ease and confidence with which individuals can assert their identity improves economic efficiency and social cohesion", and vice versa (Crosby, 2008, p. 4). Yet such levels of data collection would have had effects far beyond increasing public services efficiency. As Lips, Taylor, and Organ (2009b, p. 834) argued at the time, "new digital [identity] systems may not only bring about benefits to government agencies", they can also be "expected to lead to significant changes in the relationship between the citizen and the State". Over the remainder of this chapter, we will consequently unpack these changes in greater detail.

5.4.1 State Surveillance

From the outset, campaigners feared the government had less than noble reasons for increasing citizen legibility, with potentially grave effects for liberty and privacy. Primarily, the NIR seemed to provide the technical foundations for a "visionary if not audacious" expansion of the surveillance state[76] (E Whitley *et al.*, 2014, p. 208). With hindsight, the NIR was "an obvious technology of surveillance" (David Barnard-Wills, 2012, p. 2). Not only did scrutiny of the scheme reveal that law enforcement would be able to access the database at will, but it also transpired that officials in national and local government, and even some private sector actors would be able to query the NIR (Wills, 2008, p. 168). This only magnified initial privacy and security fears, which Ministers then struggled to quell. As identity expert Adam Cooper explained, the final nail in the coffin came during one especially heated Parliamentary debate. One of Blunkett's main arguments for the scheme, playing up the entitlement and security

[75] The drive for transparency also manifested in greater visibility for citizens of what government was doing. The Office for National Statistics, for instance, was formed in 1996 to help inform policymakers by collecting, organising, and analysing data in an impartial manner. But it also published data that could help make government accountable. At the same time, the workings of government were 'opened up' through the introduction of freedom of information (FOI) requests and the establishment of the National Audit Office to help hold government to account. Together, these changes promised to make government more responsive to citizens' needs and more willing to share data on how it was supporting them. "Sunlight", as American Judge Louis Brandeis poetically put it well over a century ago (1890), "is the best disinfectant".

[76] Parts of government even ended up publicly recognising this, as the epigraph that leads this chapter attests.

angles, was that the NIR would help the police and security services identify, track, and intercept terrorists and other criminals. This was all well and good. However, as Cooper pointed out, in disclosing this Blunkett had inadvertently drawn attention to how easily the same powers could be turned on any enemy of the state, however broadly construed. And this, in turn, raised questions about the possibility for misuse by officials, for instance by 'bad apples' surveilling or stalking innocent individuals. Civil society groups—like NO2ID, Big Brother Watch, and Privacy International—consequently deployed Blunkett's own arguments for the scheme against it, to great effect.

From a political-philosophical point of view, this surveillance-related concern breaks down into at least three issues. First, there was the immediate risk to privacy stemming from misuse of the NIR's surveillance apparatus by government agents. Thanks to the sheer amount of sensitive data being collected, a power imbalance would have been created between officials and data subjects. This, one might assume, would have been headed-off through appropriate regulation and governance measures. Yet, amazingly, government did not appear to have implemented many such checks and balances. Researchers at the LSE (2005, p. 195) found that access by the police and other security actors would have been almost entirely "covert" and so essentially "unconstrained" in practice, and that privacy protections were therefore "so weak as to be virtually useless". Even proposals for an 'audit trail'—recording whenever an identity was verified, along with the reasons why records were accessed by officials—did little to address the issue, as the aforementioned covert action would not have been captured (Wills, 2008, p. 171). This effectively gave law enforcement carte blanche to surveil individuals, with close to real-time tracking of where cards were being used and for what purposes. And unscrupulous officials could have even used the database to surface (and potentially even alter) people's sensitive personal data, without their knowledge or consent. The LSE's report consequently raised the very real possibility of NIR employees impersonating innocent people registered in the database, with little scope for restitution or accountability (LSE, 2005, p. 196).

It almost goes without saying that this is bad security practice. Nothing destroys trust in a digital system quite so fast as allowing officials unconstrained access to personal data. By contrast, Estonia's digital identity system explicitly encourages citizens to review logs of who has accessed their data, and why (Trikanad, 2020, p. 6). Citizens can then raise complaints with an official's superiors if anything untoward appears to have occurred. This brings us to our second point. Radical transparency of the Estonian sort, accompanied by clear routes for rectification, could have helped limit the scope for abuse of the NIR—if, for instance, New Labour had properly implemented a functioning audit trail system. This is because, rather than creating a tool for covert state surveillance, the Estonian approach retains a focus on individual rights and entitlement. Digital identities in Estonia primarily grant citizens access to the goods and services of the welfare state. Their purpose is thus not to give the state power over citizens, but rather to empower citizens. Additionally, Estonia grants

citizens the novel right to query those with insight into their identity records. Such protections, philosopher Carissa Véliz (2024d) has suggested, demonstrate the well-established link between transparency and trustworthiness: betraying the common belief that the "more transparent an entity is, the less wrongdoing it is able to hide, and the more trustworthy it is supposed to become." We might therefore see this as the 'good' side of surveillance—a way for citizens to address the power imbalance such systems can create by allowing them to surveil agents of the state from below.

However, in lieu of such protections in the British context, we must consider the effects of increased legibility for relatively powerless citizens; a point that inverts the last. As Jeremy Bentham (2001, p. 277) argued centuries earlier, "the more strictly we are watched, the better we behave". Bentham (2010) accordingly described a system of control for use in a hypothetical prison, premised upon the indeterminate threat of constant but unknowable observation by agents of the state. As Michel Foucault (1980, p. 71) later elaborated, this panopticon amounted to a new "invention in the order of power" that drew on the deep connections between seeing, knowing, and governing. As inmates did not know whether or not they were being watched at any particular moment, they would self-discipline and generally act as if they were being watched—a more subtle form of control than the physically coercive tactics states have historically employed. The link with the NIR as a surveillance and control system should therefore be obvious. Disciplinary effects for individuals' personal liberty would have stemmed from knowing that the state was monitoring their actions, much like East Germans experienced with the Stasi (Macnish, 2015). But citizens' freedoms would have been especially 'chilled'[77] by the NIR thanks to the fact the system was digital, and tracking them across the public and private sectors (Lyon, 2009, p. 45). After all, the 'unblinking eyes' of a pervasive digital panopticon would surely have led to more pronounced disciplinary effects than those that a manual, paper-based bureaucracy could ever have achieved.

5.4.2 Citizenship and Balance

New Labour's proposals therefore betrayed a shift in the way that the British state viewed its citizens. As Higgs (2011, p. 200) argues, after 9/11 large parts of government had "a purely negative lack of trust in the population". We can consequently see why there was an "increasing desire to pool information in order to profile them to establish risks" (Higgs, 2011, p. 201). But the country had, several times in the past century, already rejected such centralised state surveillance and control on

[77] Such chilling is admittedly hard to quantify. Although there is little empirical evidence of panoptic 'chilling effects'—a recent and useful exception comes from (Hadjimatheou, 2023)—the concept has primarily been taken up and developed by neo-republicans, close cousins of liberals. Please see Chapter 8 for more. But, if the NIR truly was a technology of surveillance, as Barnard-Wills claims, then its contribution to an arbitrary capacity for state domination of precisely this sort seems quite clear to me.

the grounds that it criminalised law-abiding people (Rolph, 2004). The government accordingly faced an uphill battle. However, from the very earliest stages of Parliamentary debate, it became clear there had been "very little deliberation […] about the details of a Bill that could fundamentally alter the relationship between the citizen and the State" (EA Whitley & Hosein, 2010, p. 79). In particular, the scheme would obviously have jettisoned Britain's intentionally-decentralised administrative approach. No longer would citizens therefore have been able to take comfort in the fact that, say, HMRC were, in important ways, partially obstructed from liaising with the Home Office about their personal situations. Implementing a persistent, unique identifier would have provided the state with an easy way to join-up databases at the backend, and brought most of the dealings people had with the state under one all-seeing system. This was a key motivation for the scheme. And, as cards were to be "obligatory" for "active citizenship"—and required to realise the "benefits of liberty"—there would be few places to hide should citizens not submit (Rose, 1999, p. 240).

Government did not shy away from this. In an increasingly insecure and globalised world, New Labour argued, some reduction in liberty was a necessary evil (David Barnard-Wills, 2012). Particularly when it came to foreigners, the state explicitly pursued "a security policy that considered aliens as a political and military risk" to be controlled via identification (C Reinecke, 2009, p. 64). It believed that their reduced privacy and liberty was a price worth paying for preventatively identifying terrorists and criminals (Fuchs, 2013, p. 684). But it was not only aliens that would be affected. A 'more appropriate' trade-off between security and liberty would also need to be struck with citizens. Soon after replacing Blair as Prime Minister, Gordon Brown (2007) reiterated this point in a speech discussing "the relationship between the private individual and the public realm", where he talked openly about needing to find "the right balance" between "protection" and "opportunities". What Brown was suggesting amounted to a radical rebalancing of the social contract. He argued that government needed "a more secure way of establishing and protecting people's identity", including using "biometrics to identify false passports" and "deny terrorists and criminals financial freedom and the ability to move across borders"—and, as somewhat of an afterthought, to "provide more personalised public services" (2007). Identity cards would therefore help arrest the freedoms of those the state did not trust, but were also a way to achieve freedom through the state and its welfare apparatus.

However, whilst talk of better 'balance' was common, with hindsight it is clear that liberal states of many stripes did not manage this balancing act well (Véliz, 2024b, p. 125). Whistleblowers have revealed how extensively citizens were monitored by governmental mass surveillance programmes throughout the 2000s (Lyon, 2014; Stahl, 2016). In the name of national security, this information was used to discriminate against people's freedoms with little in the way of legal recourse, fairness or accountability (Hintz & Brown, 2017). More concerningly, surveillance state thinkers have also shown how such intrusions were relatively easily justified by liberals, as

nothing resembling harm, interference or obstruction appeared to occur if citizens were merely surveilled and profiled (CJ Bennett & Lyon, 2008; Neocleous, 2007; PT Smith, 2020). Citizens were, after all, still 'free' to act in the classical liberal sense, even though they were under panoptic levels of surveillance. If you have nothing to hide, the saying goes, you have nothing to fear. Indirect appeals to chilling effects were, and still are, consequently some of the only arguments classical liberals could offer when pushing back against the securitisation narrative—arguments with severe limitations (Hoye & Monaghan, 2018). And, with terrorism threatening the liberal way of life more generally, sacrifices seemingly had to be made—recalling arguments previously made only in wartime. After all, preserving privacy to support the development of freedom of thought will always be important in a liberal democracy, but securing basic liberty tout court must take priority.

We can, however, question the security narrative, even granting that some reduction in privacy may well have been required. Most obviously, the NIR's database would have made an extremely appealing target for hackers and fraudsters, given the quantity of sensitive personal data it would have brought together (EA Whitley & Hosein, 2010, p. 147). The scheme could therefore have ironically ended up undermining both security and privacy by opening up new attack vectors for criminals. And identities, if stolen, could have been used to perpetrate all sorts of crimes. Criminals and terrorists were not the only concern, either. Such drastic surveillance would have "decrease[d] the protection individuals have against state incursions" (Véliz, 2024b, pp. 126–127). Security from the state, after all, is one of the other foundational premises of liberalism. John Stuart Mill, for instance, held that "there is a circle around every individual human being which no government […] ought to be permitted to overstep" (Mill, 1900, p. 443). And, in pursuing security at such a high cost to privacy, government was likely over-stepping. Jennifer Chandler (2009, p. 138) has consequently contended that many post-9/11 schemes, including identity cards, amounted to counter-productive exercises in 'security theatre', that undermined their own ends "by introducing new vulnerabilities or by sacrificing the security of a minority for a feeling of security for the majority". Identity cards certainly seem to fit this bill. The relationship between citizens, aliens, and the state would have been distorted to such an extent by the scheme that something distinct about British liberalism was in danger of being lost (Agar, 2001).

5.4.3 Scrapping Identity Cards

By 2010, with a General Election looming, the prospect of a centralised digital identity programme had accordingly become decidedly politically toxic. Public opinion on identity cards had turned (YouGov, 2010) and, as all opposition parties had pledged to undo the scheme (E Whitley *et al.*, 2014, p. 207), the issue was soon decisively resolved. Shortly after forming a government, the Conservative-Liberal Democrat Coalition announced that tens of thousands of identity Cards already in circulation were to be scrapped, with the NIR decommissioned and its hard drives

shredded (Home Office, 2011). This was primarily framed as an urgent civil liberties issue—pushed through as the very first legislative action of the incoming government. The Coalition Agreement (2010) pitched the move as a way to "reverse the substantial erosion of civil liberties under the Labour Government and roll back state intrusion." Although David Cameron and Nick Clegg did not countenance a full return to Thatcherism or even classical liberalism, they nevertheless decried 'big government' (Ruth, 2011, p. 75) and aimed to shrink the size and influence of New Labour's "command state" (Nick, 2011, p. 54)—primarily by dismantling what they saw as the centralised lynchpin of its embryonic digital government. As the incoming Home Secretary, Theresa May, put it, the Coalition wanted "to reduce the control of the state over decent, law-abiding people" (Home Office, 2010); a clear reassertion of the classically-liberal notion of freedom from the state, in the wake of New Labour's attempts to institute freedom through the state and its identification-based welfare apparatus.

Despite hundreds of millions of pounds having already been sunk into the scheme, the budding experiment into centralisation and legibility was consequently finished. Or so it seemed. In reality, parts of the programme would quietly live on. Although the domestic population was shielded, physical cards and a digital database were retained—and subsequently expanded—for purposes of immigration control, in the form of 'Biometric Residence Permits' (BRPs) (Nayar, 2015). There is a cynical historical circularity to this outcome. Much as asylum seekers had been the first to be issued identity cards by New Labour, migrants would remain the only group managed via cards retained under the Coalition. British identity policy thus slotted back into a familiar historical groove, with mandatory identification reserved once more for foreigners alone. In line with how the state had treated aliens throughout the twentieth century, entitlement would have to be proved, regularly and often, for anyone the state saw as 'other'. And, just as traditional forms of identification had raised inclusion issues in the Windrush scandal, BRPs would go onto generate similar effects—especially for individuals' dignity. Indeed, studies have found that the scheme reminds migrants of their 'difference', can make them feel unwelcome, under the threat of panoptic, digital surveillance, and even criminalised (Warren & Mavroudi, 2011). It is therefore not a stretch to think some British citizens would have felt similarly, if identity cards had been retained for the entire population. BRPs give us a fascinating glimpse of a Britain that could have been, had the election been resolved differently.

5.5 Normative Conclusions

Despite the failure of identity cards, New Labour's time in office nevertheless heralded a pivotal moment for British identity systems. There was now cross-party consensus that the state's traditionally paper-based bureaucracy had become inadequate for dealing with the spiralling fraud issues that remote authentication in the public and private sectors had unleashed. As public expectations around the

efficient provision of online services kept growing, digitalisation was now also seen as necessary and desirable—as we will see, the Coalition just disagreed about who should be responsible for driving this change. Yet, in the meantime, the problems that identity cards were intended to fix would remain unresolved. Departments still urgently needed new ways to securely identify people, with the local, face-to-face interactions that had historically sufficed now well and truly depreciated. At the same time, the piecemeal documentary approach was fuelling genuine inclusion issues. With centralised digital solutions off the table, however, and no replacement for identity cards imminently forthcoming, the Coalition effectively left individual departments to unsystematically continue 'digitising' their siloed, legacy systems, while enforcing an austerity logic that removed the very funding needed to support more transformative developments (Margetts & Dunleavy, 2013, p. 5). Predictably, this resulted in yet-more functionally-redundant, decentralised systems, with the limited addition of web portals representing minimal attempts at modernisation. Britain accordingly remained stuck on firmly Chango's first path, with new designs for a genuinely digital identity system seemingly required.

Some experts I talked to consequently lamented that such a big step forward for state digitalisation had been derailed by vague threats of lost liberty and overbearing surveillance—particularly when so many other countries have since handled similar transitions without lurching towards dystopia. Benjamin Welby, an ex-civil servant and OECD identity expert, expressed particular frustration with the "libertarian narrative, which of course people buy into, because it's […] a very simple one. You know, government overreach, government surveillance, government can know everything you're doing; isn't it terrifying, isn't it awful?". He queried what really would have changed as a result of identity cards, given that government already held so much of this information, albeit in an "incoherent", "unjoined-up", and "messy" mesh of systems. I must admit some sympathy with this view. But I would suggest that New Labour's identity card plans were more problematic than similar foreign schemes. As Windrush's hostile tracking, democratic exclusion, and even deportation of legitimate citizens demonstrated, a lot was politically, socially, and ethically at stake in Britain when it came to changes around identification (W Williams *et al.*, 2020). Rights, liberties, and even citizenship were already being unfairly removed from marginalised populations under the documentary identification regime, demonstrating just how disastrous identity exclusion had become under the modern state system. And the digitalisation of identity would have granted the state even more central power, control, and oversight—threatening to extend the state's distrust of the 'other' to the entire domestic population. This confirms to me that such systems are deeply entangled with the state's ability to filter, socially sort, and discriminate.

Of course, this may well have been acceptable as part of a wider revision of the social contract. But while increased identification and legibility after the World Wars had been a price worth paying for public goods like National Insurance and the NHS, as their repeal made clear, many of the equality and welfare advances made under

New Labour did not, in fact, hinge on identity cards (Powell & Powell, 2008). Instead, the state's primary focus was clearly on securitising the citizen-state relationship, with the perceived distrust and criminalisation of normal, law-abiding citizens poorly received by the public (Higgs, 2004, p. 187). Underpinning this was also the idea of one, person one identity: or, as Chango (2022, p. 8) puts it, "the notion of authoritative identity credentials as a monopoly of the government". Later schemes we will discuss rowed-back on this, allowing people to use different identities in different contexts, but NIR was entirely inflexible. Government had consequently tried to assert itself as sole arbiter of formal identity truth—a far cry from the flexible autonomy over their identities that all citizens had enjoyed just a century earlier, and some had once again experienced in a resurgent form on the internet. Even though fixing identity in terms that the computerised state machine could understand would admittedly have made identifying, policing, and sorting the population easier (David Barnard-Wills, 2012, p. 134), fundamentally tying a wide range of public and private services to a central digital database ultimately proved to be unacceptable. New Labour's proposed changes to the social contract were rejected; and its high-modernist ambitions were extinguished.

Chapter 6.

Federating Digital Identity Systems in Britain

> "The [overall] mission of GDS is about the digital relationship between the user and the state, and how we can make that a more seamless experience, how we can build once and build well—rather than building multiple times—and reducing duplication"
>
> *– Tom Read, former Chief Executive of GDS (quoted in Glick, 2021b)*

Having dismantled the identity card scheme, yet inherited the issues it was meant to solve, the Coalition government set about finding a new path through the rubble. The result would be a genuinely world-leading experiment in public-private collaboration—and the state's second big attempt at digitising identity. Reviving an idea that had found limited traction under New Labour, the Coalition took the novel decision to *federate* the nation's governmental identity apparatus. This was a direct rejection of the increased central legibility and surveillance of identity cards had necessitated. Instead, a new system—*GOV.UK Verify*—was designed, by a new, digitally-focused organisation, around the concept of private sector partners delivering identity verification services on behalf of the state (GDS, 2014a). The scheme thus constituted a bold trial, at least at the nation-level, of both a relatively untested technical architecture and governance structure. For the first time, official identity was to be assured through the market, for profit; though government would retain an important regulatory role. And although Verify, like identity cards, ultimately failed, subsequent governments have made clear that its federated model will continue to define our digitally-mediated relationships with some of Britain's most important institutions (Prime Minister's Office, 2024b). Verify accordingly provides the ideal case for exploring the normative implications of this architecture for governmental digital identity.

In this chapter, I evaluate Verify through the familiar lenses of liberty, equality, and citizenship, again combining interview data with evidence from the literature. I begin by foregrounding similar schemes that preceded it in the private sector. I then detail how federation came to be implemented in a governmental context—focusing on how and why shifting to a public administration setting alters the normative impacts. What becomes clear is that, despite being the product of a 'digital'

department, Verify failed to trigger the paradigm shift around identification it was intended to catalyse. More importantly, I also argue that—under both the Coalition and subsequent Conservative governments—there was a concerted, ideological effort to make enjoying the fruits of citizenship depend on the intermediation of identity by corporate actors. This was largely done for privacy reasons; a reaction to the perceived overreach of identity cards. Yet although Verify addressed surveillance and control worries, I nevertheless argue that the resulting 'privatisation' of identity reflected a concerning shift in the state's understanding of citizenship—and that exposing formal identification to the vagaries of the market was exceptionally risky. Indeed, the scheme's inclusion results turned out to be catastrophic. This should give reason for pause when it comes to subsequent governments' renewed commitments to the federated model of identity provision, and sets the stage for my attempts to square the circle in the following chapter.

6.1 Identity without Centralisation

The challenge the Coalition faced in 2010—finding a replacement for centralised governmental identity provision—was not unique to the British state. Globally, and across multiple sectors, organisations of all shapes and sizes were struggling to reliably identify and authenticate the people with which they needed to interact online. Although our focus so far has primarily been on state identification systems, we will therefore briefly consider some of the private sector systems that had emerged throughout the 2000s. After all, as previously discussed, internet use was booming. And achieving the robust and remote authentication of all those users had become a pressing problem for many businesses offering online services (Kerr *et al.*, 2009, p. xxiv). But while the British state had pursued identity cards as a country-wide solution to this problem, other organisations opted to build bespoke systems to solve their own issues. These businesses had consequently come to hold centralised, digital records on their customers and/or employees (Chadwick, 2009, p. 3). By the time identity cards were scrapped, many internet users therefore held numerous online accounts; with the companies they shopped with, for forums and other entertainment sites they frequented, as well as with the systems their employers used to control access to corporate networks. These companies were all effectively maintaining their own proprietary, smaller NIRs—central, unified stores of user data, sometimes even containing detailed biographic and identity information. A familiar problem had consequently emerged.

As identity expert Phil Windley (2005, pp. 8–9) explains, these systems all employed the same basic processes with which we are already familiar. First—if required, as many early online services operated pseudonymously or even anonymously—an individual's identity claim would be vetted via an *identification*

process[78]. Users would then be issued with an account and access credentials. Thereafter, whenever a credential was presented, an *authentication* process would give the organisation some level of assurance that the person accessing a system had the right to do so. This generally relied on one of three techniques. The most popular, you will recall, involved demonstrating 'something you know', like a PIN or password. But other factors could also be evaluated, including 'something you have', such as a token or device, or 'something you are', such as a biometric signal (Kent *et al.*, 2003, p. 46). In the most secure systems, combining these techniques in a multi-factor authentication (MFA) process would help deter fraudulent access, by increasing the complexity of any required deceit (Y Wilson & Hingnikar, 2019, p. 15). Finally, if successfully authenticated, the individual would be given *authorisation* to proceed; granting them access to an account, allowing them to change some information, or enabling them to make a transaction. "The problems haven't changed", as identity fraud expert David Black explained to me—these basic processes have been essentially solved (technically) for decades, but getting the "meta layers" of governance, support, and privacy right is always the real challenge.

As we know, however, companies were not handling these challenges very well, particularly when it came to authentication (Higgs, 2011, p. 178). Although four decades of research had illustrated the drawbacks of passwords, Corbató's invention remained the main method by which most organisations protected users' accounts (Bonneau & Preibusch, 2010). This was despite the fact that passwords offer a bad customer experience and were known to be negatively impacting organisational security (Dmytrenko & Nardali, 2005). An authentication crisis was consequently unfolding, with rampant password reuse and poorly-protected personal data generating high rates of identity theft and fraud (Price, 2008, p. 97). Yet some companies noticed a business opportunity here. Just as government had attempted to solve these same issues via identity cards, some of the most powerful corporations in the world tried to emulate the strategy in a corporate context. Microsoft's *.NET Passport*, first released in 1999, is the prime example (Chadwick, 2009, pp. 10–11). Much like an identity card for the internet, Passport was intended to replace the multitude of authentication and identity management systems across the web with a unitary single sign-on (SSO) solution, backed by—what was then—the biggest technology company in the world (Microsoft, 2000). And Passport had a big advantage over identity cards. Rather than being confined to Britain alone, Passport would have brought the benefits of straightforward identity management to the entirety of the internet—at the cost of global reliance on a multinational corporation.

[78] Identification could have proceeded in person or remotely, and would have been carried out to differing degrees of certainty depending on the risks involved. Signing up for a supermarket reward card, for example, may require very little in terms of identity assurance, but banks have a legal duty (called Know Your Customer or 'KYC' regulation) to perform more thorough proofing.

However, for much the same reasons that New Labour's NIR had drawn criticism, Passport was likewise lambasted by much of industry and civil society. Most notably, Passport was a similarly "centralized system with a single point of attack and failure" (Oppliger, 2004, p. 23). The safety of users' data, as well as that of any organisations relying on Passport, would therefore depend on Microsoft keeping it safe. But numerous security issues with the system were identified (Kormann & Rubin, 2000; Oppliger, 2003). At the same time, Microsoft was (rightly) seen as trying to install itself as the monolithic and monopolistic provider of identities and authentication services on the internet, which did not sit well with powerful consumer privacy groups. Thirteen of these groups consequently raised a suit with the US Federal Trade Commission, contending that Passport empowered Microsoft to a) monitor what its users were doing, b) potentially charge exorbitant fees for its monopoly services, and c) deny users choices over which providers to use for proving their identities online (Dmytrenko & Nardali, 2005, p. 637)—all of which went against the web's libertarian ethos in much the same manner as identity cards. Centralisation was, in this different context, thus also firmly off the cards. Instead, a safe, easy-to-use, and scalable alternative was required, that could solve the same problems as centralised systems without replicating their downsides. The federation of identity—a key technical development—was, and still is, the primary way in which the nascent identity industry responded.

6.1.2 Federated Digital Identities

Ironically, the federated counter-movement can also be traced back to Microsoft. It was Kim Cameron, an identity trailblazer, that crystallised many of the problems with centralised digital identities in a short but influential paper, published a few years after he joined the company. In The Laws of Identity, Cameron (2005) provided a high-level outline of the problem space, and popularised the notion of the internet's 'missing identity layer' he had been developing since the 1980s. When it came to centralised schemes, like Passport, one 'law' amongst several Cameron (2005, p. 7) held was that "[d]igital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship". In other words, when accessing Microsoft services, he thought most users would accept needing a Microsoft account. But, "it did not make sense […] for Microsoft to be involved" in other companies' "customer relationships"—users were not "clamoring for a single Microsoft identity service to be aware of all their Internet activities" (Cameron, 2005, p. 7). And much the same was true of identity cards. Powerful institutions, in both scenarios, had effectively inserted themselves into situations in which they did not belong and, in doing so, could learn too much about users and the services with which they were interacting. People felt that their personal data was being disclosed to unnecessary and unjustified intermediaries, which contributed to the systems' respective failures.

So, how would a federated alternative operate? The problem, for Cameron, boiled-down to a question: how could the 'relying party' (RP) in a digital interaction trust that any particular individual—a 'subject' or 'entity'—was who they said they were? His solution was to rely on an 'identity provider' (IdP) specialising in identification[79]. The so-called 'standard model' of digital identity—which imagines a trust-triangle between these three entities—was born, and to this day persists as the principal identity paradigm (S Wilson, 2022b). Under this federated model, each and every organisation does not control their own centralised database of user records (Fishenden, 2005, p. 9). Instead, several separate databases, run by different organisations, might exist, but would all be recognised and trusted by actors across the network (Chadwick, 2009, p. 3). This would allow individuals to create identities with the organisations of their choosing and, crucially, reuse them across different contexts—another 'law' (Cameron, 2005, p. 9). For instance, many people today maintain credentials with one or more of the Big Tech platforms[80], which they can use to log-in across many different websites. And although these are not full-blown identities, they nevertheless convey the benefits of federation. Users are given choices about where to store their data and, by the same token, organisations offloads the risks associated with handling personal data to companies with established and mature identity infrastructures. But if a user does not want, say, Microsoft to know they are logging-in to a particular service, they are free to use another IdP; they are not locked into using any one, monolithic provider.

In a typical federated identity transaction, then, an individual presents an identity to an RP that, in turn, consumes it. The role of IdPs is consequently to issue, exchange, and revoke identities to enable this process (S Wilson, 2011). They administer specialised identity systems, organising data, linking them to individuals, and helping them manage their identities over time. But they do no more than this, staying out of customers' relationships with the businesses they are accessing. Federation is accordingly meant to ensure that different digital identities are not needed for every single organisation with which an individual has a relationship (Chadwick, 2009, p. 3). Ideally, as mentioned, identities would even be interoperable, with mutual trust architectures and open standards meaning that individuals could use identities created for one purpose in other contexts, or even port them between identity providers (Fishenden, 2005, p. 10). This was meant to make life simpler for individuals, while also making their online interactions more secure—not least because they would be less likely to (re)use poor passwords across a litany of logins and accounts (E Whitley & Hosein, 2010, p. 210). And, for businesses, securely managing a multitude of potentially sensitive identities and personal data, along with complex

[79] This provider could be internal, like the IT department of a large corporation, but the role was likely better played by a dedicated company possessing the technical know-how to assure the legitimacy of claimed identities.

[80] More specialised IdPs, like OpenAthens, Shibboleth, PayPal, or Disqus, are also relatively common.

technical questions of verification and authentication, could now be outsourced to companies specialising in such services, leaving them to focus on their own specialisms; be it providing news, information, video streaming, or shopping facilities. Federation consequently saw rapid uptake in the private sector, with whole ecosystems arising around open standards like SAML, OAuth, and OpenID[81].

6.1.3 Initial Takeaways

The promise of federation is certainly compelling. But there are a few initial takeaways here. First, we must recognise that the technologists developing federated systems were primarily concerned with identity in corporate settings (Windley, 2005, p. 11), so had paid little attention to the social issues that could potentially emerge from the technology's wider uptake. Indeed, as Windley (2005, p. 13) notes, it was all-but assumed that the relationships between individuals and these systems were to be "dictated on the terms of the business or organization and consented to by the individual". But this straightforward, contractual context is distinct from the far more normatively-contested struggles over state identification we have thus far discussed; this was not identity as a tool for increasing state legibility or even as a proof of citizenship. Instead, federated systems were primarily developed as a technical solution, informed by computer scientists' perspectives on the narrow problem of remote identity assurance in commercial environments (S Wilson, 2011). The level of meaningful consent being achieved was thus low. So long as an individual needed access to a system, say while onboarding at a new employer, they simply had to accept the IdP's governance terms—though we know vanishingly few people ever read such terms and conditions (Marotta-Wurgler, 2012). Whether this 'consent' is sufficient, and whether greater levels of consent can and should be designed for, must consequently be considered—particularly when federation is extended to a public sector context.

Second, and relatedly, when conceptualised through the computer scientist's lens, identification can seem almost banal. Today, we have become so used to signing-in, entering passwords, and even scanning our fingerprints and faces, that doing so has faded into the background of everyday life. Of course, technologists will then have much to say about how to better implement such systems. There will always be ways to make them run better, reduce the number of false positives, increase usability, or make any number of other such improvements. But this approach should not necessarily satisfy a political philosophy considering identity in a nation-state context. As we have seen, *non*-digital identification systems are already deeply powerful tools for political recognition, population management, and societal control. We must

[81] The Security Assertion Markup Language (SAML), OAuth, and OpenID protocols underpin most federated systems, and were originally developed by powerful industry players like OASIS, AOL, BT, France Telecom, IBM, Microsoft, Google, Verisign, Internet2, and the Liberty Alliance (Bertino & Takahashi, 2011, pp. 76–77).

accordingly guard against importing a Morozovian 'techno-solutionist' outlook from the private sector via federation—not to mention the deeper folly of Scott's high-modernism. These are not benign or neutral processes for technical experts to optimise. Identity policy is backed, in a state context, by powerful systems of administration, coercion, and control, with deeply political impacts across the different contexts in which they are deployed. Thorny issues of consent, privacy, inclusion, and security must therefore be considered, and balanced against other policy goals. What makes sense or is acceptable in a corporate setting may well not be appropriate for government usage. Indeed, once we begin thinking in these terms, the normative slant quickly re-emerges.

Third, even from this brief précis we can extract one of the most foundational assumptions made by federated identity evangelists: that each identity is a 'thing'. This stems directly from Cameron's standard model, which primes us to think of 'an' identity existing as a sort of digital dossier of information that can be compiled, stored, and passed around—somewhat independently of the actors involved (S Wilson, 2022b). This clearly aligns with the paper-based, formal identities the bureaucratic state developed in the Industrial Age. State actors needed to be able to identify people they might never have met, and this was achieved through standardised identity documents. But this was a significant—and, historically-speaking, recent—development. After all, identity before this late-Victorian shift was not reducible to the cards and records that have since been used to make populations legible. It was essentially local, relational, and performative. In Cameron's terms, the RP and IdP had therefore been one and the same person. The local publican would have decided for themselves whether or not to trust you, identifying you through a combination of your clothes, speech, and social vouches from other customers. Even when dealing with 'the state', you would have identified yourself to the king's men using his seal or signature. But a token from an unknown third-party would have been meaningless. This, however, is exactly what federation attempts to realise. Identity is made impersonal, tradable, and standardised. And this opens up space between the RP and IdP that never really existed before. The king and his men might thus no longer need their own seal, and instead can trust a third-party business to verify and assure identities on their behalf.

Once we are thinking of identity in these terms it does seem natural that a third-party could specialise in managing identities for many RPs—making markets for identification services seem entirely plausible. It makes sense that the actors involved in the standard model "hold, present, exchange, use and consume digital identities as if identity is some sort of merchantable good" (S Wilson, 2022b, p. 2). We might well also imagine that companies would and could pay for consuming properly-verified identities. As identity expert Emma Lindley agreed, "by making it a thing, we do inadvertently make it like a commodity […] and it becomes a marketplace of digital identities." But is this desirable? And what if digital identities are better understood not as things, but as services, processes, relationships, or something else entirely?

These are massive questions, which we can only begin to answer in this chapter. But I would note that Cameron's model has already drawn criticism by some in the industry. Stephen Wilson (2022b, p. 3), an identity veteran, has suggested this scepticism is driven by a growing recognition that federated marketplaces have failed to take hold in the quarter-century since Cameron outlined them—which we might have expected if digital identities are indeed goods, let alone goods with any inherent value. This has been a significant upset, not least as much capital and time has been spent attempting to sustain such marketplaces. The standard model, and ideas about marketisation more generally, will therefore need critiquing as we look closer at federation. But first, we need to understand how the British state went about implementing its own version of such a system.

6.2 Federating Governmental Identity

The rejection of identity cards in 2010 sent waves rippling through the public sector. The civil service's century-long efforts to centralise Britain's identity systems had suffered yet another setback. Not only had the political feasibility of a national digital identity system been effectively eliminated but, given how foundational remote identification is usually taken to be for digital government, many interviewees consequently argued that the decision also delayed the state's progress towards digitalisation writ large. OIX's Nick Mothershaw, for instance, suggested that, even today, lacking a centralised system still "hamstrings us […] and means we can't join things up." Ex-civil servant and OECD identity expert Benjamin Welby went further, suggesting that such a system now constitutes the "fundamental infrastructure" needed to ensure a modern "society functions". Yet the Coalition had dismantled the scheme, so an alternative had to be devised. Consensus was that a common identity solution which could be re-used across departments was still needed, even if centralisation and mandatory registration had been ruled out. The newly-formed Government Digital Service (GDS) was thus set to task on the issue and, in 2014, publicly launched its replacement, catapulting Britain to the forefront of the federated digital identity landscape (GDS, 2014a). With the advent of this new system, soon branded GOV.UK Verify, Britain became the first country in the world to pursue the federation of governmental identity at scale. We will consequently evaluate the scheme in detail.

6.2.1 Verify's Approach

So, what made Verify different? Most obviously, the scheme eschewed a central database, instead relying on numerous approved, third-party providers to independently confirm identities on government's behalf (Stalla-Bourdillon *et al.*, 2018, p. 787). IdPs in the federation were therefore trusted to control their own smaller identity databases. This was explicitly intended to lessen the risks that storing records in one system would have incurred and, at the same time, ensure that government

could not maintain any kind of central oversight over the population[82] (National Audit Office, 2014, p. 5). Increased legibility and surveillance had, after all, been among the chief worries with identity cards. Verify was accordingly built from the ground-up to be privacy-preserving. At a technical level, IdPs could never know which service a user was accessing, and government could never know which IdP a user was utilising (Glick, 2019b). This 'double-blind' approach had several benefits. Keeping IdPs in the dark stopped them from profiling users, while limiting the data government collected reduced the possibility of it later being used for ill. But involving the private sector also addressed deeper concerns, relating to government's ability to build and run such systems in the first place. Not only would relying on multiple companies avoid creating a single point of failure, but GDS (2014a) claimed that working with IdPs would make the scheme fundamentally "more secure and less vulnerable". The clear implication was that these specialist businesses possessed expertise government could not match.

Nonetheless, GDS still had to shape what private sector IdPs would be doing. By opting not to manage digital identities itself, government was handing over functions that had previously been in the state's gift; RP and IdP, as discussed, were being prised apart. Departments would therefore only ever receive confirmation that a user's identity had been checked to a particular level of assurance (LoA), and would not be able to check the details of Verify identities themselves (E Whitley *et al.*, 2014, p. 216). But this meant GDS had to ensure the LoAs they defined would work across many different use cases. They accordingly produced official guidance—Good Practice Guides (GPGs) 44 and 45—that IdPs had to follow. These documents, which covered authentication and identity verification respectively, outlined a range of different standardised profiles, along with high-level explanations of how to reach them via different kinds of evidence, checks, and technologies. Developed with input from civil society and identity experts, this outcomes-based approach was intended to allow IdPs to make the most of "constantly evolving" methods for identity verification (GDS, 2014a). So long as certain outcomes could be reached, government would not need to get too specific about how companies got there. The hope was that this would allow them to flexibly meet the criteria and innovate. Some IdPs might scan passports and run a fraud check to verify an identity, for instance, while others might amalgamate an identity from utility bills, birth certificates, and credit reference agencies[83].

As this shows, Verify's design was underpinned by a specific view of the state and its relationship to the private sector. As industry veteran Andrew Hindle put it to me,

[82] As Computer Weekly reported at the time, "Verify is designed to overcome concerns about government setting up a central database of citizens' identities" (Glick, 2014).

[83] As Higgs (2011, p. 181) notes, credit reference agencies like Equifax and Experian maintain vast databases of personal information with which they commercialise the management of identity fraud risk. Cooperating closely with the state and financial services, these private companies have been made privy to sensitive information most others will never see.

"You look here, you look at Australia, you look at North America, where the tendency is much more towards small-state, high levels of personal responsibility […] As a result of that, it's almost inevitable that you need to have private sector involvement." Indeed, delivering digital identities through the private sector was seen as essential. Several senior civil servants made clear to me that Verify's federated model was the only 'live option', politically, after identity cards. Government had to reduce its role to that of standards-setter and market-maker—a significant retreat. Some saw other motivations, though. Alexander Blandford, who worked on identity systems in government at the time, suggested the programme was driven by "the libertarian wing of the Tory Party". Evidence for this can certainly be seen in the scheme's design and governance. Although paper documents distributed by the state would remain essential for creating legal identities, Verify identities operated much more in line with the web's decentralised, libertarian ethos. Government departments received only the data needed to progress an interaction and no more, with numerous checks and balances put in place to bound the state's reach (E Whitley *et al.*, 2014, p. 216). Notably, GDS even went so far as to setup an independent Privacy and Consumer Advisory Group (PCAG) to shape its work, which included many of the most vociferous critics of identity cards[84]. At both the technical and governance levels, then, GDS tried to limit the civil service and rely instead on third parties.

However, Verify's most libertarian aspect was no doubt its deep commitment to market logics. Of course, market participation in the first place was entirely voluntary, for both companies and users (GDS, 2014a). And offline solutions remained available to those who did not wish to go digital. But users who put their trust in the newly-privatised, digital services were promised speed, efficiency, and security—"most people will be able to complete the registration process online, without having to wait for documents or instructions to be sent in the post as happens with existing services" (GDS, 2014a). GDS's faith in the market was totalising, as perhaps it had to be in a time of government austerity (Etherington, 2020). Citizens consequently had a central role to play as market actors. They decided which IdPs to sign up with and, because providers were paid per user, competition was supposed to encourage cost-savings[85], with providers pitted against one another for a share of citizens' trust, data, and any profits. And, at least to begin with, this market-making approach certainly garnered interest from the private sector. Forty-four providers initially bid to be part of the scheme, with eight IdPs selected in the first year: Cassidian, Digidentity, Experian, Ingeus, Mydex, PayPal, Post Office, and Verizon (Fishenden, 2020, p. 36). But, in another characteristically-libertarian move, rather than using legislation to define its relationships with these providers, GDS took the unusual step of setting all terms,

[84] Nevertheless, some researchers argue the scheme did not go far enough around privacy, particularly when it came to ensuring technical unlinkability (Brandão *et al.*, 2015).

[85] As more departments adopted Verify, government as a whole therefore expected to "replace face-to-face, phone and postal methods of identity proofing and verification, enabling them to automate their services' business processes" and save money (National Audit Office, 2019, p. 12).

including pricing, though commercial contracts alone. Few could consequently have doubted the new organisation's commitment to the tools of the market.

On paper, then, Verify certainly looked like it would address many of the drawbacks with identity cards, while nevertheless securing citizens' identities in online interactions. The scheme's purpose-built digital identities would clearly have addressed the binding and appropriateness problems. And its federated model should have been able to grant citizens access to all the same government services as a centralised system. The state should, therefore, have eventually been able to replace numerous existing systems with this digital alternative—not to mention realised the added bonuses of increased user choice, minimal government oversight, and a big boost to the digital economy. Over time, Verify might even have come to underpin a burgeoning digital identity ecosystem, along the lines Kim Cameron had envisioned. From the outset it was, after all, intended that identities created under the scheme would be able to interoperate across the public *and* private sectors (E Whitley, 2016, p. 23). If Verify identities were 'good enough for government', the argument went, then why should corporate RPs not also be able to consume them? In Chango's (2022, p. 6) terms, Verify would thus have represented a big step towards "digitally doing digital stuff"—though I do not wish to overstate this. Under the hood, IdPs would still have predominantly relied on paper documents created by the state using legacy processes. In theory, however, GDS was living up to its name, demonstrating how a new department could develop new, digitally-native solutions fit for modern public administration.

6.2.2 Verify's Issues

Verify, however, could not deliver in practice. Like the NIR, the scheme was consequently abandoned well before it achieved significant population coverage. Its central aim, the de-duplication of siloed identity schemes across government, accordingly failed. The reasons for this are numerous. The first warning sign was that the market actually failed to provide a key piece of Verify's technical architecture. David Rennie, who worked on identity cards and Verify, explained that GDS "couldn't get a hub, out in the market" and so were eventually forced to build one themselves. This was a crucial piece of infrastructure, that provided the matching service between different users, IdPs, and government services (E Whitley, 2016, p. 22). Although a hub-less design was considered, it was quickly set aside to avoid multiple privacy issues, including the possibility of prejudice based on IdP choice. As Rennie put it, "if you come to me with a Coutts identity as opposed to a Lidl identity […] there is an unconscious bias". The hub therefore played an active role as mediator to negate these sorts of risks, functioning as a middleman between all the different parties (GDS, 2014c). Due to Verify's privacy-centric design, however, playing the part of a hub was not very attractive to industry—little unencrypted data that could be monetised was exposed, so there was limited commercial opportunity. Right from the outset, then, market failure crept into the scheme.

GDS's market zeal should have been tempered by this early experience. Companies had made clear they would only go where there was money to be made. Yet a second, bigger problem—Verify's exceedingly low verification rates—stemmed from the very same issue. For the first few years, providers successfully verified only 38% of users trying to access Universal Credit[86] (Public Accounts Committee, 2019b), well short of the 90% GDS promised (National Audit Office, 2019). But this should not have been a surprise. As privacy researcher Phil Booth noted, "the problem with marketisation […] is that the ones with the profit incentive just go for the middle of the bell curve". This left people in the long tails—i.e. expensive edge cases—excluded. Verifying someone with a passport and credit record might cost a provider just a few pounds, while proofing somebody with no documents or footprint could cost hundreds. And many providers I spoke to were quite upfront about the fact they saw no reason to absorb those costs. Verify therefore effectively entrenched existing exclusion issues. People without passports or driver's licences would remain poorly-served, and even basic data disparities stemming from married users' previous and current surnames could often resulted in failed verification attempts (E Whitley, 2018, p. 35). This meant already-marginalised populations were, as usual, likely to be doubly-disadvantaged. The middle classes generally fared well, while young, poor, urban families, the elderly, and those living in 'rural solitude' were again left further excluded[87] (OIX, 2021).

These issues were only compounded by GDS's decision not to legislate or specify inclusion targets in providers' contracts. This effectively left them with no levers for addressing exclusion[88]. Yet characterising this as a market failure would also be unfair. The market was functioning as intended; to make IdPs money. However, GDS were not making this easy. Existing legislation covering regulated parts of the economy meant that digital identities could not be accepted in many use cases, even if RPs wanted to support them. Alcohol purchases, for instance, still require proof of age with a physical hologram (HM Government, 2003), while similar issues surround gambling, the sale of restricted goods, and financial services. But, again, GDS did not pursue legislative changes to support Verify's wider use. This led Digidentity's Dick Dekkers to flatly claim that government "blocked the reuse of Verify accounts in the private sector." To him, and others, GDS seemed only concerned with public services,

[86] Much later this rose to almost 60%, but only after years of missed expectations (GDS, 2021). Neither figure includes users who dropped out of the process early.

[87] The big difference with Verify, however, was that BRPs score very highly against GPG 45. Migrants will thus, ironically, have seen some benefit from being forced to carry biometric identity cards—even if they may have struggled to amass other identity evidence.

[88] As Nick Mothershaw pointed out, the only market-based solution would have been to allow differential pricing; to charge RPs more for proofing difficult cases. But, as he made clear, this would never have been acceptable: "you can't start categorising and pricing people on the basis of the ID documents you've got". The hub was specifically designed to prevent this kind of prejudice and market discrimination. Providers were consequently left in a financial bind.

even though they had led providers to believe that Verify identities would eventually be reusable across the entire economy (Glick, 2019b). And legislation was not the only blocker. GDS's decision to mandate proofing to the relatively-rigorous LoA2[89] meant IdPs could not 'get users in the door' (E Whitley, 2018, p. 66). Additionally, as Privacy International's Tom Fisher explained to me, on a technical level Verify identities "wouldn't work outside of government with regard to the way the matching was done". With such limited use cases, however, there were very few reasons to sign-up—which is why, instead of meeting its original target of 25 million users by 2020, Verify barely reached 6 million (GDS, 2021).

The scheme's issues did not end there. Those who did sign-up were unimpressed with Verify's design. As Jon Nash summarised, "from a user perspective it was a mess. It was like, 'here are these eight organisations, seven of which you've never heard of. Pick one at random, basically, and then give them all your personal identifying information because we don't want to hold it'". Emma Lindley walked me through signing-up for a government service. As she noted, after starting on GOV.UK, "all of a sudden you're in this convoluted sign-up […] then, after 10 minutes, you come back to the original transaction". The federated journey consequently made no sense to users. People thought they were interacting with the government, so were understandably reticent to share their data with companies who had been unexpectedly inserted into the process, away from the GOV.UK estate. Yet GDS had seemingly failed to test the federated model with early users, even though the organisation claimed to be driven, above all else, by user research (GDS, 2014b). As one senior civil servant lamented, "by the time Verify was doing proper user research, it had its hands so tied on the [federated] model by privacy" that it was too late to change course. Many other interviewees agreed. As the Public Accounts Committee (2019a) concluded, the scheme was "over-ambitious from the start" and consequently ended up fundamentally "failing its users".

6.2.3 Verify's Demise

Though providers told me they regularly complained to GDS about these issues, little changed. The normative trade-offs were locked-in; haunted by identity cards, the government had pursued privacy and marketisation at the cost of usability and inclusion[90]. GDS had, however, also failed to seed a functioning market—which was inevitable, according to identity expert Gilad Rosner, as they had "an immature

[89] Although there were plans to add a lower LoA1 route, for use on lower-risk use cases, these never materialised (GDS, 2017).

[90] This was perhaps best summed-up by a story one interviewee told me about the then Minister for the Digital Economy, Ed Vaizey. At a meeting of the all-party parliamentary group for digital identity, Vaizey reported that even he could not sign-up. "I have five incomplete Verify accounts", he said, which immediately prompted the question, "how on earth is a normal citizen meant to get through this?"

conception" of the economics of identity. For the programme's first few years, government had heavily subsidised IdPs' costs, paying providers both an initial reward for each sign-up as well as an annual fee per active account (National Audit Office, 2019, p. 18). This just about kept the market afloat, despite low uptake. But, in late-2018, Theresa May's government announced that it would be gradually passing fiscal responsibility for Verify to the programme's IdPs (Glick, 2018). Providers would "now receive a lower price for each user sign-up, with […] further price reductions in increments as user volumes increase" (National Audit Office, 2019, p. 18). And, as Verify identities were still unusable in the private sector, no replacement for this lost income was forthcoming from the wider economy. Three of the five remaining IdPs therefore promptly pulled out, reducing the 'marketplace' for identities to a choice between Digidentity or the Post Office (Glick, 2019c). Ironically, as Digidentity also facilitated the Post Office's identity checks, this effectively created a single, monopolistic database of users' identities—precisely the situation the scheme was originally designed to avoid (Joshi, 2020).

Further blows then came thick and fast. Months later, the National Audit Office (2019) published a damning report recommending Verify's termination. In 2020, the Treasury then banned any further development of the scheme, instructing departments to seek alternatives (Glick, 2020b). History thus repeated itself. For the second time in a decade, departments either began returning to their old, siloed registers, or else started planning new systems to replace another failed, nation-level scheme. HMRC set about reworking an existing system, and DWP later launched a new service based on HMRC's backend (DWP, 2020). Both had originally been intended to provide Verify's main source of users. But neither department had been able to fully make the switch due to Verify's failings. DWP were particularly burned. Cabinet Office had co-opted its flagship benefit, Universal Credit, to drive Verify's user adoption (GDS, 2012)—integrally linking the two programmes' fates. Yet, as an identity expert at DWP explained, it was immediately obvious that "Verify wasn't going to meet our demographic" due to its strict proofing requirements. Worse, each time an IdP dropped out of the Verify programme, "tens of thousands of benefit claimants" were suddenly faced with non-functional accounts or user support, as the double-blind design meant DWP had no way of finding out who was affected (Glick, 2019b). RP and IdP had been split, so no linkage between the department's records and IdPs' databases existed to even help diagnose the scale of the problem. And this was a population that was, by definition, already facing financial hardship—which, as we will see, meant identification-related delays had serious knock-on effects.

However, the great irony of the programme was that, in its death throes, Verify also revealed a glimpse of what could have been. The coronavirus public health crisis hit just as the scheme was being wound-down. And this presented a perfect cocktail of issues for non-digital systems. In-person proofing became impossible as businesses and Jobcentres closed, while people were confined to their houses. As Matt Warman, then Minister for Digital Infrastructure at DCMS, argued, COVID-19 was showing

that it was "more important than ever for businesses and the public sector to adapt quickly and provide people with services online [… because proving] who you are digitally has become a vital part of everyday life" (Barnard, 2020, p. 5). The need for remote authentication consequently skyrocketed (Pelizza *et al.*, 2021), and Verify was perfectly placed to benefit. The first week of the pandemic alone saw almost 120,000 new users signed up, after massive queues initially overwhelmed and crashed the service as it became one of the only ways to get newly-unemployed people onto Universal Credit (Glick, 2020c). Verify therefore enjoyed a brief reprieve, of sorts, in its final moments—and Treasury officials even granted the scheme another eighteen-months of emergency funding (Glick, 2020a). Between January 2020 and March 2021, the scheme accordingly gained 2.5 million more users, meaning Verify eventually broke the 8 million accounts mark[91] (GDS, 2021). This did not change the Treasury's underlying view, though. The market failures and inclusion issues that had dogged Verify were considered insurmountable, and so, on the 30th of March, 2023, the scheme was finally shuttered (Burghart, 2023).

6.2.4 Techno-Solutionism/High-Modernism

Taking a step back, the collapse of Verify's marketplace was likely one of the biggest nails in the scheme's coffin. But one of the most curious aspects of the Verify saga is that GDS do not seem to have thought much about how to create a stable, competitive market in the first place[92]—even though market dynamics were central to the scheme's long-term success. Instead, following their characteristically 'agile' way of working, developing a minimum viable product (MVP) was the priority, almost regardless of the policy requirements, political context or, as discussed, user need. GDS clearly viewed digital identity as merely a technical problem to solve. I think this betrays Verify's essential techno-solutionism, imported from the corporate world which initially birthed identity federations. There are multiple aspects to this critique. First, we must recognise that the scheme's ultimate success relied on departments giving-up their existing abilities to check who they were interacting with, at least digitally, and retreat to the role of RPs in the marketplace. Obviously, effecting change of this magnitude was going to require a political fight. As Mike Bracken, GDS's founder, later identified, "Many of the people running departments fundamentally

[91] Many of these accounts will be duplicates, as there was no limit to the number of accounts individuals could have with different providers. People also will have, for instance, forgotten their details and opened new accounts. However, with no central database there is no way to tell how many unique accounts existed.

[92] Fraud expert David Black recalled an early meeting with GDS where he was asked "What's the user need of an identity provider?" He replied, "to make money for their stakeholders and shareholders." This was met with laughter, at which point Black repeated his point and reminded the Verify team that IdPs are "not a charity". Likewise, from the IdP's perspective, Emma Lindley recalled GDS's "naivety around the commercial". After being told about the pricing plans she told GDS that her company was "already heavily invested but we can't make that model work." Nothing changed as a result.

believe that the [GDS Government as a] platform model takes away their power" (Matt, 2018). But why would any mandarin give up power without good reason? GDS faced an uphill battle, and it would have been politically naive to think otherwise. Yet, at every turn, they bungled their attempts to make giving up control palatable.

Perhaps GDS thought that if they just built a good enough product, adoption would follow. But Verify's performance fell so short of the mark that this was never going to happen. A further issue was that—as OIX's Nick Mothershaw lamented—although GDS "had a team of people essentially trying to sell to government departments", they were "not sales people". The Verify team consequently promised too much while achieving far too little, *and* then did a bad job of selling the substandard product they had created; only half of the expected government departments were ever onboarded as a result (Public Accounts Committee, 2019a). As the setbacks mounted, GDS's senior management therefore changed tack. Despite not having created a solution that met departments' or users' needs, they simply imposed their product on them anyway. Much of the limited uptake Verify achieved thus relied on GDS forcing through unpopular change. In pursuing this, the strong personalities of both Bracken and the Minister for Cabinet Office, Francis Maude, were certainly useful[93]. David Black, who worked on identity fraud in government, explained that "part of why Verify failed was because the GDS management were going in with a sledgehammer—'digital by default', or 'digital by dogma' as it became known in the civil service—without really listening". Many people that I spoke to who worked in government at the time echoed this view, and did not look back fondly on GDS's early days.

To be fair, many have tried to reform the civil service. Bracken and Maude were not the first, nor the last. But the primary reason I peg Verify as techno-solutionist is that GDS showed total disregard for the complexity of the policy issues surrounding the history of British identification[94]. This was endemic in much of the department's work (Cook, 2014). Just one year after the Coalition's first digital strategy was published, a group of academics identified limited understanding of existing governmental IT systems at GDS, and a total "lack of complex systems thinking" (Alan W Brown *et al.*, 2013, p. 6). Yet, shockingly, this appears to have been intentional.

---

[93] Many interviewees from across the public sector stressed the importance of a strong Minister, and their resultant appreciation of Lord Maude. They noted that you need significant political will to get an identity scheme off the ground in Britain, which he had. David Rennie described Maude as "a great advocate" and noted that "Verify was very weakened intellectually" once Maude was moved on. Steve Pannifer echoed this, regretting that GDS lost "someone at the right level that can articulate and really […] champion the idea".

[94] As information systems scholars Edgar Whitley and Gus Hosein (2010, p. 1) make clear, identity policies introduce a "range of unique challenges […] that require distinct skills from key policy-makers"—differentiating them from more general considerations surrounding other information and communication technologies. Yet these challenges have often been overlooked by politicians and policymakers in Whitehall.

As one senior civil servant working in identity explained to me, GDS espoused "an attitude that nobody else knew anything" about identity; senior management told officials in other departments that they did not see "the point of policy officials" and that "policy doesn't need to exist". Despite a century of struggle over identification systems in Britain, and the extremely recent experience of identity cards, GDS believed that technical prowess was all that mattered—though they could not even deliver in that regard. This lack of respect for policymakers' expertise hamstrung many of the organisation's projects. *The Register*, for instance, reported on the "chaos" surrounding the rollout of GOV.UK in 2015: "GDS' newcomer status was supposed to be a breath of fresh air. In fact, the digital gurus' lack of any skills or knowledge other than webpage design appears to have equipped them poorly for the tasks in hand" (Orlowski, 2015).

What makes this all the more frustrating is that some of Verify's market failures could probably have been headed-off. After all, the civil service has regulated industries for centuries. And it is no secret that markets have a tendency to consolidate[95] (Baran & Sweezy, 1966). Accordingly, we might have expected GDS to set the rules of the game in such a way to ensure sufficient reward for companies while preventing monopolisation. This would have given IdPs reasons to play and kept the game stable. Yet, as *Computer Weekly*'s Bryan Glick explained to me, in actuality the Post Office and Experian immediately scooped up 85% of Verify's users because they were the only recognisable brands on the list. And GDS put in place no mechanisms to correct this. Of course, in a functioning marketplace people can always, in theory, look elsewhere if they are not happy with a product service (Wolff, 2011, p. 174). This is how markets develop and self-regulate. But we also know that, in reality, consumers often fail to overcome inertia—for instance, not switching energy provider when it is economically rational to do so (BEIS, 2018). GDS' decision to not pursue any market remedies to this issue, and denigrate the very policy experts that might have been able to help, is therefore especially confusing. When signing-up, users were simply faced with a drop-down list of IdPs to pick from, so naturally opted for one of the few names they recognised[96]. Rather than promoting competition and innovation, market incumbents were thus systematically advantaged. This is hardly a good way to build a strong and stable marketplace.

For all these reasons, Scott would have likely identified Verify as a high-modernist scheme, too. It has all the hallmarks: "standardization, central control, and synoptic legibility to the centre" (Scott, 1998, p. 219). GDS standardised digital identity via the

[95] As Scott (2010) makes clear, "capitalist firms are constantly striving through collusion, lobbying, legal maneuvering, and violence to establish monopoly positions".

[96] Conversely, Elinor Hull explained how Barclays did not fare well as an IdP, which prompted them to soon drop out of the scheme, because consumers were worried about their bank knowing even more about them—particularly if they were on Universal Credit. Government surveillance was evidently not the only concern; private sector surveillance worried citizens, too.

GPGs, wrestled control of governmental identity from departments, and even ran a monolithic 'data dashboard' to track progress (GDS, 2021). Although the legibility of *individuals* to the state was therefore limited by Verify's privacy-centric design, GDS certainly tried to make the rest of government submit to their totalising, centrally-managed system. As Chilson (2021, p. 52) argues, these "simplistic, reductive legibility efforts abandon information." Bespoke, nuanced identity systems were almost replaced with one-size-fits-none LoAs. Additionally, two further markers of high-modernism are the mandation of inadequate schemes and the rejection of embedded experts' practical knowledge, especially the concerns of civil society (Scott, 1998, pp. 4–5). GDS's 'sledgehammer' imposition of Verify clearly meets the first criteria. And we have already discussed the department's institutional dismissal of policy expertise. But GDS's hubris regarding civil society concerns was revealed in its approach to PCAG. As one member of the group, identity consultant David Birch, contended, PCAG was not "an advisory group, because [GDS] never paid any attention to anything they said". Gilad Rosner, another member, agreed. Almost at every turn, experience and expertise was systematically ignored, much to the scheme's eventual ruin.

6.3 The Citizen-State Relationship

We have, so far, discussed how Verify's broken market, poor user experience, and high proofing standards led to dire inclusion issues. Until now, this is the main normative concern I have raised, with choice over a user's IdP and increased privacy (from the state) the main benefits on the other side of the scales. But behind all of this sits a more philosophical concern. Verify sought to fundamentally change the nature of governmental identity provision in Britain. The scheme attempted to replace direct relationships between the state and its citizens with consumer relationships, intermediated by companies. And while some scholars, including Marion Fourcade (2021), Edward Higgs (2013), and Orsi Husz (2018), have touched on the ethical implications of other kinds of private sector identification systems, the deeply normative implications of Verify's market-centric displacement of governmental identity in Britain has never received much attention. As *Computer Weekly* reported, with hindsight one "Whitehall insider" asked, "how can it be right that the private sector was allowed to become the exclusive gatekeeper for deciding whether or not citizens can access online public services?" (Glick, 2019a). Yet I could not find anyone asking these kinds of questions during Verify's earliest days. Although the scheme ultimately failed, it is therefore nevertheless worth evaluating this central aspect of its design—particularly, as we will see, given federation's continued relevance to Verify's successors, and other schemes around the world.

Primarily, I propose that more general arguments about the consumerisation of citizenship can help shed light on the federation of governmental identity systems. Under Verify, IdPs were paid per transaction, while individuals were empowered to make 'choices' in a marketplace. But this relies on a very particular view of freedom

through the market, and lends weight to arguments that the state was beginning to see its subjects more as consumers than citizens. Verify consequently connects identity policy to a wider debate around neoliberalism. For decades, successive British governments had moved away from offering quality public services themselves, "contracting out" functions to achieve "value for money" for taxpayers (Margetts, 1999, p. 144). With Verify, however, this way of thinking was extended to the country's flagship national identity system. Perhaps there is little normative salience to this point. On the service state view, we might well expect that governments should explore different ways of efficiently managing citizens' identification (Lyon, 2009, p. 48). What, though, does attending to the privatisation of digital identification reveal? I contend it adds an important dimension to the critiques I have so far raised. Verify created a conflict between companies' needs and users' needs, putting space between citizens and the state. We will consequently explore why GDS pursued a federated model, and where the impetus for the approach came from in the first place. Ultimately, this will lead me to question whether markets are an appropriate tool for distributing identities at all.

6.3.1 Verify's Intellectual Heritage

Perhaps surprisingly, Verify actually owes its genesis to New Labour. In 2006, James Crosby, a banker, was appointed by the then Chancellor, Gordon Brown, to "build on work underway across Whitehall" and "consider how public and private sectors can work together" to solve identity assurance (HM Treasury, 2006). As this suggests, third-parties have always had a hand in online identity provision for government. In fact, Verify grew out of two federated predecessors[97]. The first was the *Government Gateway*, which launched all the way back in 2001, well before identity cards, as a joint venture between the Office of the e-Envoy and an industry consortium called tScheme (Fishenden, 2020, p. 17). Under tScheme's oversight, private sector providers were accredited to provide different levels of assurance for people accessing online services—if this sounds familiar, it is because the GPGs built on tScheme's work. The other was the *Identity Assurance Programme* (IDAP), which likewise began life under New Labour as a collaboration between civil servants at the NHS, DWP, and HMPO. They, too, intended to rely on the private sector to solve online identification. Indeed, by the time the Coalition was smashing up the NIR, both systems were pretty well-developed; Britain "had nearly a decade's experience of implementing an open standards, federated identity infrastructure" (Fishenden, 2020, p. 34). GDS consequently absorbed the IDAP, rescoping the project to suit its own purposes[98]

[97] Both, in turn, can be linked to the Electronic Communications Act 2000, which laid the foundations for a federated market of credential providers (HM Government, 2003).

[98] Adam Cooper was particularly critical of this rescoping in our interview. He explained how Mike Bracken removed the NHS from the scheme to focus on central government use cases, and replaced much of the original IDAP team with GDS staffers after taking over. The former was probably sensible. The NHS is one of the best-trusted parts of the public sector in Britain, and making access to NHS

(GDS, 2011)—making Verify much more of a rebranding exercise than an original GDS product.

In adapting the IDAP, GDS were implementing recommendations Crosby had made to the last government; that any future identity assurance system should centre "consumer need" (2008, p. 3), explicitly devaluing the government's own interests, and that the "market should provide a key role" (2008, p. 38). Verify must accordingly be understood, at least partly, as a legacy of New Labour. It was, after all, Blair that started the push for privatisation, value for money, and consumerism which later Coalition and Conservative governments doubled-down on (Clarke & Newman, 2007). Users of public services were thus no longer to be conceived of as citizens, owed equal treatment by the state, but rather neoliberal consumers, owed a good service in return for their taxes (Vidler & Clarke, 2005). Indeed, Blair's "brand of neoliberalism […] paved the way to the market fundamentalism and austerity politics" of later governments (Etherington, 2020, p. 48). Crosby just extended this logic to governmental identity. While the Coalition loudly telegraphed its rejection of 'big government', 'centralisation', and 'top-down control' (Cabinet Office, 2010, p. 7), Cameron's tenure did not therefore instil quite as fundamental a shift in philosophy as his rhetoric implied. Identity cards were one obvious point of disagreement but, by and large, the neoliberal direction of travel remained constant. He built on an "ensemble of economic policies" that affirmed the value of free markets, privatisation, financialisation, and public sector austerity (W Brown, 2015, p. 28). And, most importantly, Cameron also continued the "generalized practice of 'economizing' spheres and activities heretofore governed by other tables of value" (W Brown, 2015, p. 21)—a key point to which we will momentarily return.

At the level of public administration, this means both parties were also part of the paradigmatic shift from what has been termed *New Public Management* (NPM) to *Digital Era Governance* (DEG) (Dunleavy *et al.*, 2006). Originally identified by Christopher Hood (1991), NPM captures the kaleidoscope of views that drove market-centric public sector reforms from the 1980s onwards. NPM thinkers imported private sector competition and administrative practices to government, supposedly to drive efficiencies up and costs down (Bellamy & Taylor, 1994, p. 59). Government, they held, should focus on delivering its core services, outsourcing extraneous functions—especially "informatization"—to third-parties (Margetts, 1999, p. 171). The civil service's computing ability was consequently hollowed-out, while a preoccupation with performance measurement, incentivisation, and the disaggregation and

digital services rely on private sector IdPs would likely have caused consternation. But it also meant Verify missed out on another key use case; people rarely interact with central government, but most Briton's use the NHS. The latter decision is harder to praise. It is another example of policy expertise being undervalued by GDS's senior management.

marketisation of public services reshaped the public sector (Ferlie, 2017). This was neoliberalism in full-swing.

However, by the early-2000s NPM had led to crisis. A proliferation of arms-length agencies and pseudo-markets had emerged across government (W Brown, 2015, p. 23). And NPM's excessive decentralisation and convoluted management structures had become unsustainable, leading to the inefficient duplication of work. Worst of all, in just a few short decades, the public sector had gone from being a world leader in computing to completely reliant on outsourced IT expertise, trapped in bad contracts due to vendor lock-in—perhaps best exemplified by the Horizon scandal (Brooks & Wallis, 2020). All of this was not only costly, but it failed to generate results (Kattel & Takala, 2023, p. 7). And it was particularly disappointing given that NPM had originally been intended to save the public sector money (Hood & Dixon, 2015).

An "e-government" revolution was consequently heralded as the solution (Margetts & Dunleavy, 2013, p. 2). Yet these initial efforts resulted in little more than further transfers of public funds to oligopolistic corporate suppliers, whose poorly-built web portals merely replicated the ageing, paper-based systems they were meant to have been replacing (W Brown, 2015, p. 24). NPM's siloed and inefficient organisational structures thus persisted. Real organisational change was still required—and this time had to be truly digital[99].

Such a 'quasi-paradigm shift' finally occurred in the mid-2000s with the emergence of DEG thinking (Dunleavy *et al.*, 2006). In contrast with NPM, DEG prioritised the reintegration of fragmented public services to enable their holistic and user-centric provision, as well as "thorough-going digital changes in administration" (Margetts & Dunleavy, 2013, p. 13). It called for the radical reorganisation of the public sector, to connect up the vertical administrative silos that NPM had calcified, while also instituting more flexible, 'agile', and 'lean' modes of working to reform NPM's bloated bureaucratic legacies. At a time when austerity was squeezing public sector budgets, DEG therefore offered a way out, especially "by abandoning channel choice in favour of a 'digital by default' model" (Margetts & Dunleavy, 2013, p. 12). DEG, and GDS[100], were thus part of an evolution in neoliberal thinking—an attempt to import Silicon Valley's startup culture to government. However, transitions between modes of governance are, admittedly, never clear-cut (Margetts & Dunleavy, 2013, p. 2). Identifying the interwoven strands of NPM and DEG that drove GDS, against a backdrop of neoliberal consumerism, will accordingly be necessary to illuminate my primary normative concern.

---

[99] In this context, working 'digitally' means "[a]pplying the culture, processes, business models & technologies of the internet era to respond to people's raised expectations" (Loosemore, 2017).

[100] As Fishenden (2013, p. 997) observed, the Coalition Government exhibited "a rhetoric and aspiration that is clearly strongly rooted in DEG".

6.3.2 Neoliberal Havoc and Inequality

What, then, can all this tell us about federating governmental identity? Political theorist Wendy Brown (2015, pp. 28–30), identifies four main critiques of neoliberalism: the "*havoc* wreaked on the economy"; "*intensified inequality*"; "the *ever-growing intimacy of […] capital with the state*, and corporate domination of political decisions"; as well as "the *crass or unethical commercialization* of things and activities considered inappropriate for marketization" (emphasis original). Some of these are more relevant for our purposes than others, but all are worth discussing. First, and perhaps least apposite, is economic havoc. At a basic level, over £175 million of public money was essentially wasted developing Verify[101] (Evenstad, 2020b)—a figure that does not include the capital spent by providers. But, given its low uptake, it is hard to argue that Verify's collapse had an appreciable impact on the economy as a whole. The scheme simply never reached a critical mass—though its negative impact for individual Universal Credit claimants was certainly acute. However, what continues to wreak economic havoc, even today, is Britain's sky-high rate of identity fraud (Cifas, 2024). And the lack of a national digital identity system directly contributes, as almost every interviewee reminded me. One senior civil servant explained how even just "preventing data leakage" with more secure, digital systems would mark a big improvement over companies holding "massive amounts of data on you in some dodgy filing cabinet". And, as it can take months for someone to recover from identity theft (Experian, 2019), the opportunity cost of Verify's failure is thus likely to have been significant.

The next concern is inequality. As discussed, Verify chiefly benefitted those citizen-consumers who already had adequate identity evidence, as their identities were easily proofed. These demographics were then offered a faster, digital route to public services. By contrast, populations that were unlikely to possess passports, drivers licences, birth certificates, and other evidence—due to, say, poverty, domestic abuse, or discriminatory policies like Windrush—were left relying on ageing, austerity-squeezed, offline systems. There are evident inequalities here. Taking a philosophical perspective might lead us to recognise that Verify unjustly intensified structural inequalities for already-marginalised groups (c.f. Young, 2001). Relying on the market, after all, reduced equality of opportunity for certain groups by ensuring that only some could benefit from 'going digital'. In this way, the scheme also entrenched digital inequalities—the roughly 20% of the population that had "zero" or "limited" digital skills at the time will have been especially disadvantaged (ONS, 2019). Nonetheless, by making Verify central to Universal Credit, the state primarily tied digital identification to material inequality. Not only did the poor, long-term sick,

[101] Much of the standards and governance work done under Verify has since been translated to the trust framework, as the next chapter discusses. So some return on the government's investment can be claimed.

and disabled often struggle to use Verify in the first place, but this directly delayed their timely access to welfare (Foley, 2017, p. 16). Although DWP were eventually forced to build their own, more inclusive system, Citizens Advice (2017, p. 18) thus reported how early reliance on Verify led directly "to debt, homelessness and reduced work incentives". On a positive conception of liberty, the system will accordingly have contributed to a reduction in basic freedoms.

For neoliberals, though, this might have been a price worth paying for a freer, more innovative economy. While the nineteenth century had seen untrammelled respect for negative liberty become tempered by the state's promotion of positive liberty (Freeden, 1986, p. 53), over the twentieth century neoliberals attempted to reassert the importance of freedom from the state, valorising a market-centric view of liberty (Dixon & Hyde, 2009, p. 71). These efforts kicked-off in the 1970s, as the Keynesian postwar consensus was breaking down amidst general economic stagnation and industrial unrest. Thatcherites and the wider 'New Right' responded by tracing these issues back to leftwing centralisation, paternalism, and welfarism (Rose, 1999, p. 138). Drawing on Friedrich Hayek's scepticism of 'statism', neoliberal theorists accordingly took umbrage with what they saw as the increasingly coercive and interfering state (B Williams, 2021, p. 2). They argued that excessive bureaucracy and state intervention had made the economy inefficient, and instead promoted the idea of a leaner state, wedded to the idea of free markets and individual autonomy. This was most evident in calls for lower taxes, the privatisation of public assets, and a dramatic reduction in welfare spending—all couched in the utilitarian language of economy-centric monetary policy (W Brown, 2015, p. 28). And, as discussed, many of these ideas certainly came through in the Coalition's intellectual offering (Cabinet Office, 2010). The creation of GDS must consequently be seen an attempt to slim-down the state, furthering a neoliberal agenda via DEG at the cost of risking higher inequality.

Not all would agree that GDS was essentially-neoliberal, however. Some governance scholars instead identify neoliberal logics as having been a drag on the organisation's potential. Rainer Kattel and Ville Takala (2023, p. 11), for instance, argue that GDS's "utilitarian approach to user needs […] made it susceptible to market-based logics of austerity". I think susceptibility does not go far enough, though. Austerity logics were, in fact, central to the organisation (Margetts & Dunleavy, 2024). GDS's thoroughly DEG-centric goal was to save the government money by instituting digital change and radically reforming the public sector. And each of GDS's services advanced this mission in a different way. Verify's key aim was to privatise governmental identity and, in doing so, cut costs for the Treasury and especially DWP by shrinking the welfare bill (GDS, 2012). The rollout of identity cards, by contrast, was projected to have cost tens of billions of pounds—one of the main reasons the scheme was criticised (LSE, 2005, p. 245). Realising the same benefits through the market was consequently the solution, in line with the logics of public sector austerity and neoliberal market-building. And Verify had the added benefit of furthering a

consumerist notion of liberty. Instead of mandatory, state-backed identity cards, people accordingly gained 'choices' about whether or not to join the new marketplace for identity services as free economic actors. Extending the scheme to the private sector, as GDS always promised, would then have further strengthened the market-centric value proposition, allowing consumers to reuse their identities with more RPs[102]. Yet, as we know, GDS were never able to get the scheme working in practice.

6.3.3 Corporatised Decisions and Economised Identities

Brown's (W Brown, 2015, p. 29) penultimate critique concerns "the *ever-growing intimacy of […] capital with the state*, and corporate domination of political decisions". Without overstating the power that GDS gave away corporate actors, I think we can say something here about companies taking control of identity verification for government. In particular, if Verify ceded political responsibilities to companies, then IdPs might need to be seen less as corporate actors, and more as what Elizabeth Anderson (2017) has called 'private governments'—i.e. players that are less responsive to democratic checks and balances than the state actors they have supplanted. Put another way, this helps us think about how, while the state was being reduced to a consumer-focused service provider, businesses in turn took on elements of statehood. The 'street-level' bureaucrat's power was consequently handed to companies operating at the 'system-level' (Bovens & Zouridis, 2002). This made the choices taken in boardrooms political, with the discretion of, say, a Jobcentre worker to make conclusions about the person in front of them displaced in favour of the utilitarian calculations of a profit-driven business. Formerly-relational, local forms of identity were therefore pushed even further to the margins. At the same time, IdPs were allowed to simply decide not to serve 'consumers' that were difficult or expensive to proof. While, on a corporate level, this decision might be perfectly valid, there is a distinctly-political hue to citizens losing digital access to public services as a result. And much the same can be said of IdPs pulling out of the programme. Leaving millions of benefit claimants suddenly without means to access their Universal Credit accounts should not have been acceptable, even if it made good business sense.

Part of the problem is that, while British governments since the Second World War have been expected to offer universal services (Nullmeier & Kaufmann, 2021), most companies are not held to the same standard[103]. In Verify's case, 'choice in the

[102] Ex-civil servant and OECD identity expert Benjamin Welby elaborated on this market-centric view of what he called "empowerment". He argued that neoliberals wanted as many people as possible "to be active in the economy, and that the empowerment that they're really looking for is [people being] able to contribute to the economy and society. But ultimately […] the value of doing this is about transforming interactions so that they can be more trusted—rid of fraud, higher value, lower friction—because they think there's [economic] value to be generated."

[103] Utility companies are the obvious exception, and these industries' special status is reflected by their unusual regulatory requirements. For instance, it is very difficult for an energy company to cut-off someone's supply even when faced with non-payment.

marketplace' therefore countenanced some quite egregious exclusion—a kind of corporately-motivated social sorting. Nonetheless, it may be easy to overstate the extent to which political decisions were commercially dominated. Detractors might point out how, since the earliest days of NPM, government has always used contractors to build and deliver services. And this has not generally been considered a way to skirt political obligations. Surely GDS just failed to put good contracts in place? Verify, however, went beyond contracting-out. It almost entirely outsourced the state's ability to verify citizens's identities to the market while, as discussed, ignoring the issue's political dimensions. This naive valorisation of the market certainly risked empowering private governments. Here, David Lyon's (2009, p. 64) classic worry about 'card cartels' is also relevant. Even in the identity card days, Lyon contended that the identity landscape needed reevaluating to account for the private sector's increasing importance. He was especially worried about the "oligopolization of the means of identification" by corporations working without sufficient democratic oversight (Lyon, 2009, p. 65). This now feels remarkable prescient. The effective monopoly that emerged within just a few short years of Verify's launch certainly validates some of Lyon's fears—even if, thankfully, GDS (inadvertently) limited uptake and set pricing in such a way that a cartel could not form.

This leads us to the last of Brown's critiques; and, to my mind, the most important. Underlying all the issues we have so far discussed is a more fundamental concern—that Verify involved "the *crass or unethical commercialization* of things and activities considered inappropriate for marketization" (W Brown, 2015, p. 29). Beyond the consumerisation of the citizen-state relationship, federating governmental identity also seems to promote the commoditisation of the identities *themselves*[104]. In other words, a federated approach transformed verification services from a public good that people expected from the state into a commodity service to be bought and sold, for profit. After all, adequate financial incentives and clear paths to growth had to be grafted onto the act of proving who we were to the state for identification to be made attractive for corporations. But I think we need to be wary here: formal proofs of identity should not necessarily be conceived of as commodity services to squeeze profit from, especially if this could conflict with equal respect for citizens. On the one hand, many people may not even require digital identities, despite strong market incentives to sign them up and deliver continued growth for shareholders. Yet, if Verify had taken root, a digital by default approach would have made it increasingly difficult *not* to have an account. On the other hand, the coronavirus outbreak demonstrated how robust digital identification is only becoming more vital for accessing public services. Consequently, should the market really be performing this

[104] This mirrors a critique I have elsewhere advanced in the context of online personal identity (CH Smith, 2020).

task, or is there a better way to provide these services and thereby ensure equitable access to the digital economy?

While the next chapter will offer an answer to the second half of that question, I first want to contend that there is something intrinsically wrong with the market verifying identities on the state's behalf. The philosophical idea that some things should not be bought and sold is known as the theory of 'blocked exchanges'[105] (Wolff, 2011, p. 176). The basic idea is that the market logics advanced by neoliberals can degrade or corrupt certain goods—making markets inappropriate tools for their distribution. Common examples include selling your own organs or selling love (Wolff, 2011, pp. 177–178). Now, Verify did not directly make identity verification dependent on a user's ability to pay. It was free at the point of service, with costs covered by the government and other RPs (National Audit Office, 2019, p. 19). But the need, created by the state over the past century, to stake one's claim to a bureaucratised identity before enjoying the fruits of citizenship was no doubt made into an opportunity for profit making. And it is worth noting that, from the outset, the public did not warm to this. Focus groups interviewed during Verify's development responded poorly to the discovery that commercial interests were being built into the national identification system (Brostoff *et al.*, 2013). Indeed, Cabinet Office observed this sentiment when the idea of third-party IdPs was first explored at the turn of the millennium (Fishenden, 2020, p. 15). Nonetheless, all this user testing was ignored, despite GDS's supposed user-centricity, as their hands were already tied—the neoliberal logic of the market was to be used, no matter what. But what can moral theory tell us about this strong intuition against commercialisation?

It could be that distributing identity verification services via the market is not intrinsically wrong, but has undesirable "third-party effects" that make blocking such exchanges necessary (Wolff, 2011, p. 185). Some such effects we have already discussed, like monopolisation and increased inequality. These certainly lend weight to this argument. Practically-speaking, Gilad Rosner also pointed out how "fantastically complicated" it is to make identity federations work, given the trust you need to build between RPs and IdPs that have no real reason to rely on one another. Many government departments were, after all, happy with their existing systems. Yet GDS felt gaining choice in the marketplace was important. What, then, does consumer choice add? Rosner thought this "neoliberal conception" created nothing more than further complications[106]. He concluded "it doesn't make sense, it's inapt, it is a commercial logic perspective" that does not fit with identity provision, because "government doesn't compete" and is, in fact, the source of the identity data IdPs use

[105] Jürgen Habermas' (2005) concept of colonisation, Michael Walzer's (2010) notion of separate spheres of justice, and Michael Sandel's (2012) bounding of the moral limits of markets all advance convincing arguments to this effect.

[106] When I put these ideas to other interviewees, there was not much agreement. Providers were, of course, clear that they had a role to play. But many of the freelancers I spoke to were not convinced.

in the first place. David Black made the same point: from the state's perspective, "the problem with an identity provider is it's basically taking your watch to tell you the time". While both recognised the privacy benefits of federation, they therefore denied that choice was an important enough value to justify Verify's federated design. This architecture instead opened up an unnecessary space between RPs and IdPs, splitting the latter function off from government and thereby creating room for conflict between companies' and users' needs. In effect, GDS were then pulled in two directions—and left pleasing neither group.

Yet I still see a deeper concern. The real problem with commercialising formal identity provision is that discerning who we are—who is a citizen and, therefore, what people are owed—sits at the very heart of what *the state* does. Supplanting these irreducibly political questions with an impoverished, neoliberal measure—am I, as a consumer, getting good value for my money?—consequently carves something vitally important off from the state[107]. When we stop thinking as a political community of equals, our sense of social solidarity, which is so key to the social contract's success, is amputated. Via a million marketising cuts, the belief that we as citizens "are all in this together" is undermined (Wolff, 2011, p. 189). In this way, identity is like a femoral artery. Figuring out who belongs in our community is *the* most fundamentally political question we can ask. Allowing this to become the preserve of 'private governments'—accountable to shareholders, not us—therefore amounts to a critical injury, that leaves the state losing its lifeblood, fast. Even identity veterans like Nick Mothershaw recognise how allowing someone's "core identity" to become "a priced commodity […] is dangerous". And, while Verify only commoditised verification, not our 'core' identification documents, the neoliberal direction of travel has continued unabated. The Home Office has since outsourced the construction of a digital civil registration service to the private sector (Flood, 2023). The Scottish Government has likewise rolled out numerous contracts around its own digital identity platform (Evenstad, 2018). And, as we will see, Verify's replacement made similar mistakes. Rather than this infrastructure being built for us, and by us, it is instead tendered for and delivered for profit, usually to the lowest bidder. Is there not something crass about this? Should identifying one another not remain the preserve of the state? I certainly think so.

6.4 Normative Conclusions

Whether or not you agree, the fact is that market forces attempted to hollow out the British state's identity capabilities. And GDS's introduction of a marketplace for private sector IdPs does seem, to me, to have changed something fundamental about governmental identity in Britain. We have moved beyond the tools which Torpey and

[107] As Marion Fourcade puts it (2021, p. 158), "demands for citizenship have been reoriented toward socio-technical systems that are most visibly dominated by private institutions".

Scott equipped us with, even if we can identify elements of both high-modernism and techno-solutionism in Verify. Most obviously, the state is no longer the only key player. A clear attempt has been made to reduce the citizen to "a cog in a large market-driven, purposeful machine" that can do little more than build their credit score and demand a good service in return for their taxes (Kakabadse *et al.*, 2009, p. 106). More generally, the social contract of the postwar settlement, negotiated between equal, liberal democratic citizens, has been put at risk of being commercialised. User-centric thinking has moved us away from universalism, and towards particular, discrete relationships between consumers and the neoliberal service state (Lips, 2006, p. 42). Indeed, Theresa May, the then Home Secretary, even asserted in December 2013 "that 'British citizenship is a privilege, not a right'" (Webber, 2022). And, as we have seen, enjoying one of the most important benefits of citizenship, access to welfare, was undermined by federating governmental identity. A classical split between the public and private sectors thus may no longer be analytically useful. So, from now on do we need to evaluate identity in terms of an assemblage of state and corporate actors? And, even if (for now) the state still issues most of the underlying documents that allow us to verify identities, what would it mean if this changes? Will we then have privatised identity completely?

Despite these unresolved questions, Verify's federated model looks set to proliferate on the world stage—Britain's trial of the approach has been influential, inspiring similarly federated programmes across much of Europe, Australia, and North America. As Adam Cooper, who originally co-wrote the GPGs, explained, "it's unfortunate that a lot of the things happening internationally […] have drawn from the work that's been done in the last 15 years in the UK, but the UK is not capitalising on it." With Verify's collapse, some felt we consequently risked being left behind, while some of our closest allies continued down the federated path. Nonetheless, as mentioned there is growing discontent, even in industry, with Kim Cameron's model—stable, profitable marketplaces for identities have still not materialised, despite twenty years of industry organising to bring them to life (S Wilson, 2022b). Promising projects in Italy and Canada might yet bear fruit but, until their markets have been shown to persist, the concerns I have raised about federating governmental identity—at least with such a neoliberal impetus—should still give us reason for pause. Nonetheless, one pyrrhic victory was made during the transition from identity cards. The scheme does genuinely seem to have gone against what Carissa Veliz (2024c, p. 182) calls the *Iron Law of Digitization*; that "to digitize is to surveil". Digitising identity, at least under Verify, did *not* lead to a new form of surveillance. As an outlier in an age of pervasive digital surveillance, Verify therefore at least shows us that civil

society can still rebuff some neoliberal forces[108], and has a key role to play in ensuring any future systems deliver on citizens' values.

Finally, this chapter also concludes the historical discussions of *Part II*. Surveying all that we have covered, I would note just how much the concept of liberty implicitly at play in British identification has evolved. In a little over a century, the freedom to socially perform your identity, which had persisted since the medieval era, was first restricted by the state and its limited bureaucratic systems—initially at the borders and during wartime—before eventually being reduced to a neoliberal 'choice' over private IdPs. More generally, identity, in any formal sense, now flows only from evidence issued by powerful institutions. All 'freedom' to define yourself outside of these systems has been lost. Identity has been reduced to a technical challenge, solved via utilitarian, risk-based calculations of the available evidence. The only good news is that liberal theory provides powerful tools for considering whether these developments can accord with the impartial and equal respect for citizens that it demands. And, as have seen, the results are not promising. It is not clear that the market can or should perform this function. To put it simply: if Verify's market model failed to help over half of benefit claimants prove their identities and receive state assistance, then are markets and their choices worth it? This foundering may have been due to governance errors on GDS's part, stemming from a naive and hubristic pursuit of neoliberal marketplaces. So, perhaps more competent designers would have fared better. But I have argued there are deeply political implications of governmental identity that require citizens to be seen as more than mere consumers. If we are liberals, then, maybe we should be glad that it failed. The question now is whether we can find a way forwards.

[108] This is highly unusual—and due almost entirely to the pressure civic society groups like NO2ID and the LSE Identity Project exerted on the Coalition in the wake of identity cards. Even if civil society and policy experts were then sidelined by GDS during the actual delivery of Verify, as neoliberal motivations could not be questioned, its founding can nevertheless teach us something.

—Part III—

Chapter 7.

Rationalising Digital Identity Systems in Britain[109]

> "All identity systems carry consequential dangers as well as potential benefits. Depending on the model used, identity systems may create a range of new and unforeseen problems."
>
> – *Conclusions of The LSE 'Identity Project' Report (2005)*

Over the past two chapters, I have constructed a liberal critique of Britain's first two attempts to establish a national digital identity system. This built on interdisciplinary theoretical foundations as well as insights from historical, analogue systems—both of which we evaluated earlier—to work towards a final product. We can therefore now finish the job, and ask *What would a coherent, liberal democratic rationalisation of contemporary British digital identity systems look like?* Surveying the raw materials we have to work with, however, the outlook is not positive. With the shuttering of GOV.UK Verify, the British state had twice now failed to develop a successful digital identity scheme[110]. Both New Labour's centralised surveillance system and the Conservative's neoliberal privatisation efforts had turned out to be unsuccessful, expensive disasters. All the while, successive governments had overseen "draconian" cuts to the public sector, undermining "rights to a decent standard of life" for many of the poorest in Britain (Etherington, 2020). And identity

[109] As noted in Chapter 3, I joined DSIT's digital identity team (the 'Office for Digital Identities and Attributes') in November 2023 to lead development of the trust framework. I am chiefly responsible for finalising the next publication and shaping its strategic direction. I must be clear that no views in what follows constitute statements of government policy, and any inferences or assessments are only my personal views—except where otherwise indicated. Additionally, the interviews that formed much of the evidence base for this chapter were completed well-before I took up my position at DSIT; the argument does not, therefore, rely on any insights gleaned through my professional role.

[110] Among industry, confidence had therefore worn thin. Private sector experts lamented the seeming lack of any long-term strategy, and some even publicly declared they had lost faith in government's ability to deliver a functioning digital identity ecosystem (c.f. Joshi, 2020).

systems were intimately bound-up in these austerity efforts, as a key part of the attempt to 'modernise' the welfare state. We will consequently need to make some much-needed normative alterations if we are to eventually arrive at a consistent, coherent whole.

What, then, has government been planning? Despite the failure of these two prior systems, the current suggestion nevertheless appears to be to give both approaches another go. Over the past five years, consecutive Conservative governments have pushed the civil service to develop another federated scheme out of Verify's ashes (Glick, 2020d). And, although this successor has, from the outset, been limited to private sector use cases alone this time, the state has given itself a key role to play in governing the nascent market for identity services it still intends to catalyse. This is not all. More surprisingly, a centralised, governmental scheme is also back on the cards. Due to the massive uptake of *NHS Login* during the pandemic (NHS Digital, 2022), calls soon came for the health service to grow their system into a public sector-wide identity platform (Glick, 2021c). And while the NHS, for good reasons[111], refused, Whitehall had again witnessed the value of digital-first, centralised solution. For a second time, GDS were thus set to work developing an identity system fit for a modern, digital government.

The stage has accordingly been set: centralised, public sector digital identities and a federated marketplace for private sector verification services will co-exist. One could therefore be forgiven for thinking the state has run out of ideas—on both counts, we have, after all, been here before. For our purposes, however, a welcome corollary of this blended approach is that it provides the perfect opportunity to reflect on the final (de)merits of each architecture, as well as their combination—a task that was only made more urgent when the Labour Party took power in July 2024 after a snap election (Prime Minister's Office, 2024a). Following fourteen years of neoliberal austerity, Keir Starmer's government now has the chance to chart a new course. And, while identity policy is unlikely to be among the incoming government's most urgent considerations, finding a way past the Gordian knot Labour have inherited could yet lead to genuine transformation.

Of course, there remain reasons to be wary of centralised governmental schemes. And, after Verify, there are clear lessons to learn when building marketplaces for identity services. But revising both strategies will make it possible to learn from prior mistakes while still realising any potential upsides. And the good news is that our analysis of prior systems has already brought to light some of the most important normative lodestones. These are the risks of a) central oversight and unchecked state

[111] The NHS is one of the only parts of the public sector that citizens trust. 80% trust the NHS, compared with only 35% trusting the national government (ONS, 2022). And undermining this by associating the NHS brand with other, less-loved parts of government would consequently be an unattractive prospect. NHS Login will therefore continue to serve only the health service.

surveillance, b) commercialising the citizen-state relationship via private sector involvement, and c) countenancing persistent exclusion. Consequently, this chapter completes my reconstruction of British identity policy in political-philosophical terms. On the one hand, I argue that a suitably-bounded scheme for identity verification, not identification, in central government could finally drag the state into the twenty-first century. On the other, finding a way to pursue a federated approach *without* neoliberal-logics could open-up a hitherto unexplored path, involving cooperatives and nonprofits, to assuage marketisation concerns. Ultimately, I contend that this combination of views allows me to arrive at a defensible reflective equilibrium—one which makes digital identity systems compatible with a broadly-liberal philosophy, fit for the British context.

7.1 Identity Policy after Coronavirus

The seeds of change for British identity policy were planted during the coronavirus pandemic. In its first budget, Boris Johnson's government confirmed its continuing intention to create a functioning digital identity "market" in the UK, despite Verify's demise (HM Treasury, 2020, p. 101). And, although the first national lockdown curtailed normal life just days later, progress on the project continued. A newly-formed 'Digital Identity Strategy Board'—bringing together interested parties across Whitehall—consequently agreed a formal plan, before DCMS got to work, eventually releasing an 'alpha' draft of the proposed Digital Identity and Attributes Trust Framework (the 'trust framework') for public consultation a year later (DCMS, 2021). As this betrays, DCMS wrested control of digital identity policy from GDS in the aftermath of the Verify debacle. Nevertheless, DCMS's idea was essentially to retain Verify's federated architecture while addressing the scheme's drawbacks. Private sector IdPs would thus continue competing in a marketplace for digital identification services, governed by the overarching trust framework. From the outset, however, the scheme was scoped far more tightly than its predecessor: digital identities would not interoperate across the public and private sectors, instead limited to non-governmental use cases alone. Private sector providers were not, it seemed, still considered 'good enough for government'. But, perhaps unsurprisingly, a Conservative government had once again committed to getting a marketplace for digital identities off the ground.

This was not all the Johnson government had planned, though. Also in 2020, Matt Warman, then Minister for Digital Infrastructure at DCMS, revealed his commitment "to developing a cross-government identity system focused on user need" (Barnard, 2020, p. 3). This was a reference to a new GDS product, initially called *GOV.UK Accounts*, that the organisation would develop in parallel to the trust framework. The original vision was that citizens and residents would be able to sign-in and 'personalise' their experiences on GOV.UK via Accounts, with the explicit goal of tracking which pages they visited to algorithmically suggest content and services

based on inferred needs and interests[112] (Allum, 2020). As a result, speculation mounted that an appetite had re-emerged within government for the centralised management of citizens' data and identities. After all, while positive for users' civil liberties, Verify's double-blind design had stymied departments abilities to support citizens, leaving them with little data about users. With powerful Special Advisors like Dominic Cummings now pushing for greater data utilisation across Whitehall, however, Accounts seemingly confirmed the government's retreat from this position[113]—even though it had the potential to undo much of the careful messaging around choice and privacy that had defined official communications since identity cards. Yet none of this appeared to worry the Johnson government. Accounts soon moved further in the direction of identity cards. By late 2021, the product had accordingly evolved into a fully-fledged public sector digital identity system, renamed *One Login for Government* (Lopez, 2021).

After Verify's failure, the desire to streamline government's 191 existing account systems and 44 different login methods clearly remained (Trendall, 2023). And, as mentioned, NHS Login had shown that tens of millions of British citizens were happy signing-up for a centralised governmental identity system tied to a compelling-enough use case. Indeed, with hindsight the pandemic was pivotal. Blog posts GDS published at the time show how the crisis pushed the state to rethink its relationship with citizens, illustrating how siloed, department-by-department identification solutions caused user confusion and frustration (M Taylor, 2021). In interviews, several senior civil servants told me how, especially on GOV.UK, it was just not obvious to people why they needed to identify themselves using different schemes for different public services—and that the fragmentation had become especially noticeable as reliance on state support increased during COVID-19. But there was also another side to this coin. During the pandemic, people had become more familiar with digital identities in other aspects of their lives, too. Lockdowns forced many workers to get to grips with enterprise identity solutions while working remotely, for instance—some for the first time. Most had also downloaded two different NHS apps (NHS Digital, 2022). One civil servant working in identity consequently told me how, post-pandemic, user testing found that citizens were far more comfortable using digital routes to access all kinds of services. GDS may therefore have been right to think that public acceptance for a new, centralised digital identity solution could have been higher than it had previously.

Yet One Login's announcement also raised significant questions—not least around what interplay, if any, the scheme might have with the trust framework (Glick,

[112] It first transpired during the 2019 General Election that user journeys were being tracked on GOV.UK using cookies and IP-addresses at Dominic Cummings' behest (Spence, 2019). This evolved into GDS's current plans.

[113] The government's UK Digital Strategy confirmed the intention to collect far more data, and better utilise it, a few years later (DCMS, 2022a).

2020d). In particular, one might have wondered how successive governments ended up pursuing this combination of approaches. I think about it in terms of a 'policy pendulum'. Having reached one extreme—the state offering centralised identity cards for use across the public and private sectors—the pendulum had then swung to the other with Verify. This involved government leaving much more up to the private sector, even aspects of state administration. As we know, however, both approaches failed, leaving policymakers in a bind. Without any better ideas, they thus let the pendulum swing back half way; trying to have the best of both simultaneously. This was partly a political choice. As Gilad Rosner explained, for Ministers, "there's no political upside to doing identity", which is why it is "so much easier to kick the can down the road". With five years to make a mark on the state, however, my belief is that there is a way for the new Labour government to make this halfway-house work. But, to see how, we first need to fully understand each inherited scheme. From a philosophical standpoint, after all, the current, blended approach brings together a number of deeply ethical and political issues we have already explored. Will One Login again increase individual legibility, paving the way for state overreaches? Will the trust framework's marketised approach perpetuate inclusion issues? And, will the dual follies of techno-solutionism and high-modernism again emerge, in either—or both—of these schemes?

7.2 The Trust Framework

In June 2022, DCMS (2022b) released a 'beta' draft of the trust framework, accompanied by the legislative proposals needed to underpin the project. One techno-solutionist facet of GDS's prior scheme was therefore immediately addressed. With policy, not delivery, experts now at the helm, a Bill to support digital identities in the wider economy was made a priority. However, initial progress on this front was sluggish. In addition to identity-related clauses, the Data Protection and Digital Information Bill sought to overhaul the UK's data protection framework, which drew heavy criticism from civil society (Public Law Project, 2023). Two different incarnations of the Bill consequently fell under the Conservatives. Nonetheless, Labour should reintroduce a slimmed-down version to Parliament in late-2024[114], which is expected to fair better. The new Bill will set out government's responsibilities and powers surrounding the trust framework and the marketplace for digital verification services it aims to create (Prime Minister's Office, 2024b, p. 39). Most importantly, it should include new provisions for data-sharing between government and the private sector to support identity verifications. For the first time, this will open-up public databases to private providers[115]—something that was previously

[114] This will be accompanied by a new 'gamma' publication of the trust framework, which should see only minor changes ahead of a 'post-legislative' 1.0 publication next year.

[115] A Document Checking Service pilot laid the groundworks for this, but was small in scope and uptake and limited to just a few participants as a proof of concept (Evenstad, 2020a).

illegal outside of a few special use cases. Accordingly, to keep a tight leash on providers given access to such valuable data, the Bill will also create a new governance function within the civil service. This body will oversee the scheme and ensure that only trust framework-certified providers, accredited by third-party auditors, can take part in the ecosystem and access government data (DCMS, 2023).

The trust framework's stated aim is to "enable a secure and trusted digital identity market"[116] (DCMS, 2023). The scheme will therefore cover a wide range of commercial services: everything from eligibility checks, to consumer-facing digital wallets, and financial services products. As we know, the basic technical challenges here have been essentially solved for decades. Products offered under the trust framework should therefore suffer from neither the binding problem nor the appropriateness problem—they have, after all, been explicitly designed for private and secure identity verification[117]. But finding a way to allow government, providers, and relying parties across multiple sectors to all trust one another, and especially identity claims, is the truly knotty problem; one that is relational rather than technical. The trust framework consequently attempts to build an interlocking scaffold of legal, technical, and governance measures to assure trust in these relationships (DCMS, 2023). This is intended to give parties throughout the ecosystem confidence in the identities and attributes managed under the scheme. For the public, this means visible government backing and a recognisable 'trust mark' to help customers identify properly-certified services. For providers, this involves government mandating standards and policies it considers best-practice—including following updated versions of the GPGs developed for Verify—as well as a certification scheme. Taken together, these measures are taken to lay the foundations for a trustworthy, widely-adopted digital identity system.

At this point, it is worth noting that the trust framework leaves far more up to the private sector than Verify ever did. Excluding the costs of querying government data, pricing, for instance, is left entirely to the market—eschewing Verify's central rate setting (DPDI, 2024). Again taking an 'outcomes' and 'rules-based' approach, the GPGs and other standards only define the kinds of identity and authentication

[116] As this shows, the stated benefits of adopting digital identities across much of the private sector have remained essentially unaltered from those first proposed by the Central IT Unit (2000) around the turn of the millennium. In the call for evidence launched at the beginning of the trust framework project, Cabinet Office and what was then DCMS (2019) argued:

"If we could securely and easily prove our identity, or something about ourselves, it would help support innovation, reduce fraud and cost, safeguard our privacy and streamline online services. Whether opening a savings account, buying age-restricted products or paying tax, proving identity should be simple, private and secure."

Indeed, these purported benefits also closely resemble those touted by Verify and other digital identity schemes the world over. And, even after five more years of development, much the same upsides are today listed on DSIT's explanatory pages about the trust framework.

[117] I discuss the inclusion problem in regards to the trust framework and One Login later in this chapter.

processes that are likely to meet different thresholds for confidence—with providers and RPs left to decide what will suit their needs (DCMS, 2023). A basic eligibility check, for instance, might require just a few pieces of evidence, while opening a bank account might require far more. This allows the trust framework to cover numerous use cases, avoiding the issues that stemmed from Verify's limited LoA2 support. The use of open and interoperable standards is also encouraged, along with a raft of compulsory, user-focused rules around privacy, inclusion, data protection, and identity repair (DCMS, 2022b). But I must stress that most decisions about specific technologies are left entirely up to providers. So long as particular outcomes are achieved, providers are free to adopt completely different approaches, leaving space for innovation as the market evolves[118]. In other words, the trust framework attempts to form a kind of public-private partnership (c.f. Hilvert & Swindell, 2013). It melds corporations and a public sector governance function together, with the intent of realising a jointly-delivered market for identity and attribute verification services using data sourced from industry and the state.

7.2.1 Whose Values?

Fifteen of the experts I spoke to praised DCMS's overall approach, suggesting the decision to set minimal 'rules of the road' in the trust framework and leave much of the detail up to companies has been well received. Industry figures, especially, seemed pleased with DCMS's focus on doing only 'what government can do'. As one senior civil servant put it, there is no longer a feeling, like there was with Verify, that government "is going to just come up with its own thing without any reference to how it works out there." This is all well and good for industry, but might still give us reason for pause. There is, particularly, a danger that government may have been a little too deferential to some stakeholders. To address long-standing complaints about Verify not respecting commercial realities, DCMS explicitly pursued a novel 'open policymaking' approach with the trust framework. This has involved "working in partnership" with a range of industry groups and companies, balanced to an extent by engagement with regulators and civil society (DCMS & Office, 2019). The motivations for this are largely defensible. We do, after all, live in a democracy—and it was good to see DCMS drawing on diverse views when designing policy, not least to avoid repeating Verify's techno-solutionism. Furthermore, as decades of neoliberal cuts and outsourcing removed technical expertise from government, some degree of open policymaking was arguably needed to help avoid missteps. But it may also have left the policy-focused team inside government struggling to balance technical

[118] The trust framework could consequently end up creating an ecosystem that is not truly federated, after all. Most providers are assuming a federated outcome, but the rules theoretically encompass other approaches (e.g. distributed or even decentralised models) that would not rely on federation per se.

industry feedback with competing viewpoints. Private sector influence was undoubtedly strong.

Perhaps the best evidence of this is that, to begin with, select industry actors were actually embedded *within* DCMS. Various interviewees privately raised concerns with me about the identity consultants that initially joined the trust framework team to lead on its technical development. During the project's first few years, these consultants drafted parts of the framework almost entirely autonomously, and peer-reviewed much of the work carried out by the wider DCMS team. Yet industry concerns around possible "corporate capture"—which Jon Nash and Joseph Spear both explicitly raised with me—eventually forced DCMS to reevaluate. The consultants were consequently re-contracted externally, and kept at arms length from future policy decisions; though retained unique access compared to many other stakeholders. And this was not an isolated incident. Similar concerns around undue closeness also led to government pulling out of a long-standing partnership with the industry trade body, OIX, where DCMS had previously occupied a board seat (OIX, 2023). Any appearances of favouritism for a particular group threatened to undermine DCMS's efforts, given the importance of trust in the whole ecosystem. The department's attempts to walk the line between open policymaking and corporate capture are therefore interesting. While it could have designed the trust framework behind closed-doors, the legacy of two failed identity schemes pushed civil servants to rely unusually closely on identity experts—despite the reputational risks this forced them to grapple with.

To DCMS's credit, they also regularly tried to make room for public opinion. This included a public consultation at the programme's outset, which built a preliminary evidence base and generated the principles that went on to guide the programme. That said, the initial call for evidence only received 148 responses (2020), with only 270 responses to the subsequent full consultation (2023). The respondents also skewed sharply towards experts working in the digital identity space. Given the relatively low response rates from 'normal people', it is consequently hard to say how far public opinion was reflected in evidence gathered early on in the project. Nevertheless, a later, independently-run 'public dialogue' involving 96 members of the public also informed the trust framework, and provided a normative corrective to industry interests (DSIT, 2024b). For instance, the dialogue's findings were used to reassert the importance of values such as privacy, transparency, data protection, and inclusion in the face of industry complaints about onerous rules that would limit business prospects. Yet I do not want to overstate these effects. These findings came late in the trust framework's development, which implies many decisions had already been made without this evidence—though, of course, as the programme continues to develop perhaps these views will come through eventually. Additionally, concerns around garnering lay input for such technical work were addressed via participant

education during the dialogue process[119]. This raises the spectre of 'leading the witness', meaning it is difficult to evaluate how far unalloyed public concerns were taken into account.

7.2.2 Avoiding High-Modernism

On balance, then, there is certainly some cause for concern that the trust framework kowtows to the digital identity industry. But is this not a necessary consequence of the complexity of identity policy in modern Britain? Identity cards aside, successive governments have repeatedly pursued a federated blend of private and state actors (Fishenden, 2020). And, generally speaking, this collaboration has some obvious advantages, as we have discussed. By this point, many providers will also already have built business relationships with relying parties. They will consequently know better than government how the identification needs of, say, the Post Office will vary from those of DBS providers—so it makes sense to consult them on the rules by which citizens may prove who they are across different contexts. This is surely necessary for a multi-sectoral, public-private approach. Indeed, recall how Scott stresses that responsiveness to the practical knowledge of experts is required to avoid high-modernism (Scott, 1998, pp. 4–5). But such an approach may also seem needlessly complicated and fraught when compared to the simplicity of relying on a universal governmental identifier, where negotiating these sorts of interrelations is not always needed. After all, a 'gold standard' governmental identity would not require the blended governance structures that Britain has arrived at after decades of trial and error; relying parties would simply trust the government's processes. Conservative governments of a predominantly neoliberal persuasion have, in other words, repeatedly pursued 'the hard route', given the apparent political toxicity of centralised identity systems in Britain.

I think there is something worth praising here. And, further to Scott's point, we have already seen how both identity cards and Verify ignored on-the-ground realities, attempting to project simplified models and solutions onto the complexities of the world as it really exists. Identity cards underestimated the concerns of civil society, while Verify failed to properly consider the needs of individual government departments and the private sector. After two high-modernist, techno-solutionist disasters, it is therefore strikes me as a good thing that the trust framework tries to

[119] Given the technical nature of digital identity, DCMS argued a lengthy public dialogue process was required to fully educate respondents and avoid ill-informed concerns. For instance, any consultation on the issue always attracts fears around identity cards, even though the policy had been off the table for over decade and a half. Even if naive concerns had to be corrected, however, the question then still arises as to how far these can still be considered public opinions. Regardless, DSIT deserves praise for attempting to bring people into the process, despite all the attendant difficulties. I should also note that I was momentarily one of the 'experts' involved in the public dialogue. However, once I was offered a full-time role on the trust framework team, I stepped back from the dialogue process to avoid a conflict of interest.

avoid repeating similar mistakes. Furthermore, Scott would also have been pleased that DCMS has not mandated usage of the trust framework. Beyond respecting practical knowledge, this is another way he tells us to guard against ill-fated social engineering projects (Scott, 1998, p. 5). Indeed, the trust framework carries the specific caveat that "government is committed to delivering these benefits without the need for a national identity card. This means people will have the choice over if, when, and how they use digital identities" (DCMS, 2022b). As this demonstrates, DCMS wants to unlock the benefits of digital identification without risking any accusations of authoritarianism. The trust framework is entirely optional. If a certified solution works, presumably the hope is that people will choose to adopt it, without coercion. Making room for choice of many sorts, then—over companies getting certified, an individual's selection of provider, and their decision to actually use trust framework services in the first place—should therefore be commended. But can the same be said of One Login?

7.3 GOV.UK One Login

One Login's development has been broadly contiguous with that of the trust framework. The scheme's overall aims should, by now, also be familiar: to reduce the unnecessary costs of duplicative systems by delivering "a single, ubiquitous and simple way for people to log in and prove their identity when accessing online [HMG] services" (Cabinet Office, 2022). As this suggests, One Login is really at least two interlinked systems. After launching the basic single sign-on (i.e. authentication) element in October 2021, GDS quickly turned its attention to a bigger challenge—identity checking. This would need to be flexible enough to replace a myriad of existing identity processes across government; no small feat. But, encouragingly, initial tests proved successful, with a citizen-facing smartphone app soon following in August 2022 (Jones, 2022). And, in the years since, a modest variety of small public services have adopted One Login. However, the programme still has a long way to go before becoming the government's universal digital identity system. From Verify's travails, we know how lofty a goal this is, and so it is worrying that some of the largest departments, like DWP and HMRC, have still yet to fully embrace GDS's newest solution (Trendall, 2024b). Indeed, Cabinet Office (2022) was wary of this risk from the get-go, and warned GDS that any delays risked departments seeking other options. The One Login team are therefore scrambling to get the product to a point where it is able to fulfil the needs of some of Whitehall's most widely-used services.

On the upside, you could say, at least government now holds all the cards. Unlike with Verify, GDS are the sole identity provider this time, so do not need to accommodate private sector IdPs' commercial needs. They can instead focus on building a product that works for government—a definite advantage. But do not be deceived. While One Login has been developed for the public sector, it is in fact being built primarily by the private sector, at no small cost. With a budget projected to reach £305 million by 2025, almost all technical delivery of the scheme has been outsourced

(Infrastructure and Projects Authority, 2023). Consulting giants Deloitte and PA Consulting secured multiple contracts to build the app itself, while One Login's identity-checking, biometrics, and anti-fraud components are sourced from companies like iProov, Yoti, Experian, and Synectics Solutions (Hersey, 2023; Trendall, 2024a). Despite initial appearances, then, One Login (like the trust framework) continues the neoliberal trend of removing technical expertise from government, relying on private sector identity proficiency in a characteristically-DEG manner. Of course, I have just suggested this could well be necessary given the complexities of the modern digital identity landscape. But it means there are more commonalities between One Login and the trust framework than first meets the eye—not least because most of One Login's component providers are also certified under the trust framework (DSIT, 2024d). In both cases, then, government has decided to cede the actual construction of identity systems to the market.

The similarities do not end there, though. More positively, GDS have likewise signalled their commitment to user choice and privacy; they have ruled out mandating citizens' use of One Login—at least for now—to avoid any accusations of 'implementing identity cards by stealth' (Lopez, 2021). GDS will also allow people to use multiple One Login accounts, associated with different email addresses, despite this rendering the scheme's name a contradiction in terms (One Login Support Team, 2024). This is intended to reassure people that, say, Home Office will not be able to access DWP data tied to a particular account. Additionally, at least in theory, people will be able to choose whether or not to use One Login or existing paper-based identification routes—even though cash-strapped departments will have few incentives to keep these old routes open if One Login performs (Glick, 2021d). Generally speaking, however, all of these attempts to give users a degree of choice and privacy have been welcomed by civil society—though this is perhaps surprising, given that the scheme utilises precisely the unique, persistent identifiers which have historically been anathema to privacy campaigners (GDS, 2024). Yet there is one big distinction between One Login and the trust framework. Where the latter governs a wide range of identity products, so does not define a level of confidence those identities must reach, GDS have had to be more prescriptive. They are, after all, creating a one-stop-shop. GDS have therefore had to decide what a 'good' identity for all government departments and use cases looks like. And, as Verify demonstrated, building a universal system of this sort is not remotely straightforward.

7.3.1 Population Coverage

One of GDS's thorniest problems has accordingly been that One Login needs to cover essentially the entire population to be useful. As they themselves point out, even 99% coverage would exclude around 750,000 people (Andrews, 2022). Yet this butts up against the almost inevitable trade-off between population coverage and confidence in an identity; a version of the inclusion problem. While a single sign-on service can take a user's self-assertions as read, so is inclusive of anyone with an email

address, GDS aim to prove users' identities at a 'medium' level of confidence (LoC) under GPG 45; with less robust 'low' confidence identities possible as an undesirable fall-back[120] (Andrews, 2022). The problem is that, much like with LoA2, both options rely on individuals possessing a high-quality photo-ID—a passport, driver's licence[121], foreign identity card, or BRP (GDS, 2024). But, as we have discussed, these forms of evidence are expensive and lack full population coverage. Although One Login will not suffer from the blinding or appropriateness problems, then, GDS will have to find new, cost-effective, and inclusive means of identifying people. Otherwise, One Login will only work for those who already have sufficient identification. And, while it certainly will make these people's lives easier, it will leave the ID-challenged behind once more—increasing (digital) inequality just like Verify. As one senior civil servant at the DWP explained to me, this could be a big barrier to their department's adoption of the scheme; One Login could again end up compounding exclusion if it prevents those most in need from getting timely support. Having been badly burned once, DWP are consequently nervous.

GDS are, of course, aware of this issue, and trying to address it. Part of their solution involves the Post Office and its contracted identity provider, Yoti. Postmasters can offer people who are less confident using digital routes in-person support (Say, 2023). But this does not nullify the issues with relying on photo-IDs, which people still need via this route. The more promising solution GDS is pursuing accordingly involves the Digital Economy Act 2017, which enabled greater data sharing amongst public bodies, and should thereby broaden the range of evidence GDS can draw on to verify a One Login identity (Cabinet Office, 2023). This, at least in theory, will allow for two new checks. First, when someone uploads a scan of, say, their driver's licence, GDS might one day be able to query the DVLA and directly check their details. This should make the system more efficient and fraud resistant[122], but will not boost inclusion. Second, and more relevantly, the Act allows GDS to source a range of identity attributes from other departments, such as the DWP or DfE, with which people may already have a relationships. This could help GDS build up enough of a picture of an individual to trust that they are who they say they are, without relying on photo-ID. But both capabilities are currently entirely speculative. The infrastructure and agreements required to get these data flowing do not yet exist.

---

[120] This latter option, which relies on using knowledge-based questions and is broadly-similar to LoA1 under Verify, may get users who lack sufficient identity evidence through the door, but cannot give GDS much confidence in who they are. To be used by higher-risk government services, these identities must therefore be uplifted to medium (i.e. LoA2) via the verification of additional identity evidence.

[121] Driver's licences do not actually meet the same evidence strength scores as identity cards, BRPs, and passports under GPG 45, so it is not clear how GDS claim that all these forms of evidence can be used to reach a medium confidence level in the first place.

[122] The emergence of generative AI systems like 'OnlyFake' that can forge convincing fake driver's licences has been particularly well-reported (Cox, 2024).

And significant testing, especially around the new fraud and privacy risks this could create, will be required to make sure any new identity data sources are fit for purpose and can be trusted.

So, for now at least, One Login will not meaningfully better the inclusion rates of prior or existing systems. Beneath its digital sheen, the system relies on the same old, outdated identification processes that have held Britain back for the past twenty years. One Login is consequently, in its current guise, less transformative than it first appears. But, if GDS do ever manage to get cross-governmental attribute sharing working, then this could all change. A properly joined-up government might, at last, be able to identify individuals inclusively, capitalising on the masses of data government already holds on us. *This could be truly revolutionary.* If GDS ever successfully build such a functionality, One Login could finally end the British state's reliance on a morass of physical documentary evidence that was never intended to support general identification. We might no longer need to gather together evidence from so many sources; utility bills, bank statements, and driver's licences could be used, once again, for only their intended purposes. Potentially, it might also even nullify the need for checks with private credit reference agencies, at least for public-sector fraud prevention, as similar data could be sourced from across government[123]. And, as almost all citizens interact with the state at numerous points throughout their lives, millions of people who currently struggle to sufficiently prove their identities would newly be able to draw on their existing relationships with different departments to create a One Login and become digitally included. This is the promise of unlocking cross-governmental data flows.

The scheme could thus still turn out to be the Britain's first truly digital national identity system, finally meeting Chango's (2022) terms. Government departments would be able to move away from both the recommender system[124] and document cross-checking in favour of GDS-built data checks. But although this is an exciting prospect**,** it is worth reiterating how promissory it all is. None of the infrastructure needed is in place. And, as we know, GDS repeatedly over-promised and under-delivered with Verify. It is consequently through this lens that I suggest we should consider GDS's recent proposals to add a 'wallet' or 'vault' functionality to One Login's feature-set (Say, 2024). This could allow individuals to store various digitised attributes and credentials—such as a mobile driver's licence, parking blue badge, or fishing licence—in their One Login account, for easy access. This would be far more secure than physically carrying around these documents. If and when departments ever build out the capability to generate such credentials, this feature could thus be

[123] Here I am thinking of the Metropolitan Police's Amberhill programme, which has faced funding troubles in recent years but would be perfectly placed to monitor identity fraud.

[124] GDS have repeatedly suggested they want to make vouching part of One Login, though this has not materialised due to the fraud risk extensive vouching could open-up. In practice, then, the recommender system does not exist under One Login.

genuinely useful, even if it raises the rather inelegant possibility of people needing to maintain both a One Login 'wallet' for public sector credentials alongside a private sector equivalent created under the trust framework[125]. But all of this should also remind us how GDS's agile design approach can lead the organisation to chase exciting new features before getting the basics in place—One Login's evolution from data analytics tool, to single sign-on, to identity service, and now possibly wallet, might thus give us reasons for pause, particularly given the fundamental inclusion issues the programme faces.

7.3.2 High-Modernism, Redux

What we may be seeing with One Login, yet again then, is precisely the kind of scheme that Scott cautioned us against, once more tinged with Morozovian techno-solutionism. Of course, the basic point here is that translating people into data enables their more efficient and effective management (Kitchin, 2014). But such rationalising projects alone do not doom a scheme in Scott's eyes—this is only the first of four criteria he cautions us to watch for. The other three are a high-modernist outlook, an authoritarian state forcing through change, and a prostrate civil society (Scott, 1998, p. 5). On the first point, like any governmental identity scheme, One Login clearly risks being high-modernist. It attempts to replace a messy patchwork of analogue identification systems with an all-encompassing, well-ordered, digital alternative. In this ambition, however, it has not so far succeeded. As discussed, the system is not yet truly digital; it has not yet even managed to supplant photo-IDs, and so does not do anywhere near enough yet to ensure inclusion. It thus impressively repeats the mistakes of both the analogue world *and* GDS's last attempt at solving the problem. Additionally, Ministers have been saying for years that One Login will be forced onto departments to ensure uptake (Glick, 2021a)—even if departments like DWP see only downsides to abandoning the perfectly functional systems they already have[126]. If this happens, it means we can again identify part of Scott's penultimate criterion in action. But claiming these as the actions of an authoritarian state could be a little harder.

Nonetheless, the final years of Conservative rule arguably did see a tilt towards authoritarianism. Four controversial policies come to mind. First, there was the Treasury's (2023) exploration of Central Bank Digital Currencies (CBDCs)—a form of digital cash that will cryptographically tie funds to their owners' digital identities. Plans for CBDCs have accordingly raised privacy, surveillance, and control concerns

[125] GDS will not, after all, want to be held liable for allowing a user to present something like a fraudulent airline boarding pass. And, as I discuss later, neither are they likely to want to provide identity assurance for private sector services involving 'sensitive' products like pornography or weapons.

[126] DWP's second attempt at Universal Credit, sans Verify, successfully pays nearly 96% of claimants on time—a staggering demonstration of how much more inclusive multi-channel identification systems can be (Freeguard & Shepheard, 2020).

(Big Brother Watch, 2023). Second, 2023's Online Safety Act attempts to regulate various 'online harms' via a number of means, including age gates across much of the internet. Many people will therefore soon need to use digital identity or facial age estimation systems to regularly prove their ages online, with campaigners arguing this will restrict freedom of expression and privacy (ARTICLE 19, 2022; Burns, 2021). Third, the DfE has been sharing children's data with DWP since 2016 for fraud prevention purposes—which has triggered ICO reprimands and the head of the Association of School and College Leaders to identify an "Orwellian drift towards […] a Big Brother state" (Whittaker, 2024). Fourth, and finally, 2022's Voter Identification Regulations mandated the presentation of photo-ID at polling booths for the first time in Britain, leading to accusations of voter suppression (The Guardian, 2021). These fears appear to have been well-founded, as the requirements demonstrably disenfranchised many of the ID-challenged—political exclusion that was especially hard to justify given the lack of evidence of any widespread voter fraud in the first place (Francis, 2023).

Across all four of these examples, the state has thus made various civil and political liberties newly dependent on access to adequate identification, while citizens' expectations of privacy—particularly when using digital technologies—have been repeatedly reduced. The Conservatives do consequently seem to have launched an assault on citizens' digital freedoms, and even the right to vote. Whether or not this makes them authoritarians, it does create a difficult context within which to build public trust in two new digital identity systems. It also arguably makes the privacy-preserving, choice-based approach of One Login and the trust framework the exception rather than the rule in recent digital policy. Both were, after all, launched in the context of a 'unified data strategy' that aimed to accelerate the British state's digital transformation (DCMS, 2022a). And, as critical technologist Lauren E. Bridges (2024, p. 9) has put it, rather than reassuring the public that their data would remain safe, private, and secure, the Conservative's data strategy instead reimagined data "as an untapped resource to be exploited by industry and shared between different sectors of society" (Bridges, 2024, p. 9). In particular, she claims it sought to maximise the free-flow of data, "facilitated by frictionless infrastructures, commercializing academic research for industry use, promoting data flows between regions, and loosening data privacy laws" (Bridges, 2024, p. 9). Consequently, from a privacy-centric vantage point there are at least prima facie reasons to distrust the last government's decidedly-neoliberal attempts to digitise identification against a backdrop of state overreaches.

In sum, successive Conservative governments have done very little to build the conditions needed to help two new identification systems thrive; public trust in government as a whole has plummeted in recent years (ONS, 2024). The result is that DSIT and GDS are now operating in a difficult political context, likely making the rollout of these two systems more of a challenge than it might otherwise have been. However, with all this in mind, is it not surprising that identity policy has generally avoided the headlines? Many interviewees told me they were amazed that One Login,

and to a lesser extent the trust framework, had not attracted more criticism during development and testing. Indeed, outside of the professional computing press, and a few special interest groups, neither scheme has received much public attention at all[127]. Even the protest I got caught up in was relatively minor, and barely made headlines. And this is all despite the fact that the government has, for years, been attempting to bring digital identification into the mainstream—with the state asserting its place at the centre of both flagship solutions in a way that it would not have dared since the rejection of identity cards. Nonetheless, with a new government now in power, there is a real chance to start afresh, and potentially address many of the concerns I have just raised with each scheme. Having fully understood the inherited context, and all the complexities of contemporary digital identity policy in Britain, we can now finally turn to my preferred way of rationalising the situation, to chart a more coherent way forwards.

7.4 Squaring the Circle

Throughout this project, you will recall my goal has been to develop an account of where "to go, starting from here, which is of course what the government needs to know" (Wolff & de-Shalit, 2007, p. 11). Before advocating for change, I therefore had to explain how we got 'here'. This reconstruction was necessary to bring to light the most important judgements and principles that have emerged as drivers of my thinking throughout the reflective equilibrium process. But it should now be clear that a series of views relating to liberty, equality, and citizenship—set against a general liberalism—have played this role. And the good news is that, in terms of the received

[127] Responses to last year's consultation on the DEA to support One Login were, however, overwhelmingly negative. GDS accordingly discounted around a fifth of responses as 'out of scope'. These primarily included template emails from privacy campaigners, which admittedly did not engage much with the substance of the consultation, referencing identity cards and the Chinese social credit system. Even excluding these responses, though, public sentiment was scathing. Three-quarters of in-scope responses disagreed that GDS's proposed changes would "improve or target a service to individuals", "provide them with a benefit" or "improve the[ir] well-being" (Cabinet Office, 2023). And only a shockingly-low 2% thought the changes were likely to achieve these goals. People's main worries concerned "the erosion of data privacy and protection, data security against cyber attacks and a general mistrust in government use of personal data" (Cabinet Office, 2023). And, for most respondents, these risks outweighed any potential upsides. Respondents generally seemed to have little faith that departments such as the Home Office or the DWP would not end up using access to earnings data from HMRC to, for instance, deport people or remove their benefits. Yet the responses to GDS's proposals for greater inter-departmental data sharing were even worse. 93% of respondents disagreed with plans to increase the number of departments sharing attributes about people with GDS, with a further 87% disagreeing that the attributes GDS wanted access to were appropriate for identity verification in the first place—with many noting strong reservations around the sharing of special category data and sensitive information (like income). Whether or not such concerns will come to a head now the programme is gathering steam therefore remains to be seen. But, to me, the responses certainly suggest much of the public does not support One Login's transformation into a truly digital identity system.

position Starmer's government faces, current plans fair reasonably well on all these fronts. However, several outstanding causes for concern remain which, if constructively addressed, can yet point towards an even more coherent resolution. Before that, though, I must mention some recent political manoeuvres. In the past year, both GDS and DCMS have been involved in 'machinery of government' changes. First, under Rishi Sunak's Conservatives, DCMS's digital capacity was split-off and merged with science and business teams across Whitehall to form the Department for Science, Innovation and Technology (DSIT) (Prime Minister's Office, 2023). Just over a year later, Labour then announced that GDS and a few other technology-focused agencies would also be joining DSIT, bringing more of the state's digital capability under one roof (DSIT, 2024c). This means that, for the first time since Verify's early days, civil servants working on the state's national digital identity policies will all report to one Ministerial team.

Additionally, Starmer has pledged that Ministers will stay in post for the next five years (Hayward, 2024). This may not sound momentous. But Ministerial turnover was incredibly high under the Conservatives—between 2010 and 2023, there were eleven DCMS Secretaries of State and twelve Ministers for Cabinet Office. These constant reshuffles no doubt impacted the development of coherent, holistic policy. As one senior civil servant admitted to me, "an overarching strategy" was noticeably "absent". Relatedly, Benjamin Welby noted that "[w]hen you have something like identity, it's important to have someone like Francis Maude who's sitting at the table; but it's […] vastly more important that you've actually got consistency". Identity, with its complex history, is a difficult brief. Should Starmer keep his promise, he could consequently generate just the kind of stability that DSIT needs to make progress rationalising British identity policy. This could even involve some quite radical developments. The new government could, after all, decide to pursue a completely new solution, given its long runway. But Labour are more likely to double-down on One Login and/or the trust framework[128]. The new Secretary of State, Peter Kyle, has already said as much—while explicitly ruling out national identity cards (C Smyth & Sellman, 2024). I think this is the more straightforward path. It recognises that neither One Login nor the trust framework is really new, in any meaningful way. Each iterates on what has come before. And perhaps there is something to be said for this. Gradual improvement based on precedent fits well within a realist liberal philosophy—and accords with the precepts of reflective equilibrium.

Nonetheless, from what we have discussed, issues with both schemes remain. With One Login's creation having stemmed from a renewed desire for citizen

[128] Departments with existing systems, like the NHS or DWP, could even become IdPs themselves, recognising each other and private sector actors as both providers and RPs. Whether Government could fairly compete with industry whilst also trying to regulate the market would be an open question, but the bigger risk is that this could drag Britain back to the pseudo-markets, duplication, inequality, and artificial 'competition' of the worst days of NPM. I therefore do not favour this model.

legibility—and following significant state interference in citizens' lives during and since the coronavirus pandemic—the normative stakes of centralised identity's re-emergence could not be higher. The protests mentioned at the outset of this thesis also show how, in the minds of some, digital identities remain tied to fears around government oversight, overreach, and control. This certainly needs addressing. At the same time, Kyle's continued commitment to the trust framework betrays Labour's apparent belief in the need for the market to help citizens prove their identities, at least in some situations—which, as we know, still represents a big shift from the status quo. Labour will therefore continue trying to popularise identification as a commodity service, with potentially significant implications for inclusion. And, although One Login aims to centralise public sector identity provision, it too depends on many of the same private sector actors—not least to build the software and hardware the scheme relies on—meaning it could suffer from much the same issue. Regardless, as I have hinted, there is at least one way to square this circle. And it requires us to address persisting issues around each of the three key strands of liberty, equality, and citizenship. Over the remainder of this chapter, I will consequently explain my preferred way to weave together a coherent, liberal whole from the systems and context Labour have inherited.

7.4.1 Public Sector Identity

Beginning with the public sector, I think Kyle is right to have ruled-out identity cards from the off, despite pressure to the contrary from party grandees like Tony Blair (Morton, 2024; Wheeler & Pogrund, 2024). Defending a new, foundational identity register is simply not a fight that needs to be had. For centuries, the British state has functioned without one—and, in some quarters, distrust of such centralised databases and mandatory registration does seem endemic. Add to this that another monolithic scheme is sure to face civil pushback, as the privacy lobby has made clear, and there do not seem to be many upsides (c.f. Big Brother Watch, 2023; C Smyth & Sellman, 2024). This, of course, means I have moved quite far from my original enthusiasm for national identity cards. What I now consider to be far more useful and defensible are systems that make digitally proving who we are and things about ourselves easy, secure and reliable. But by this I do not mean that we each need *a* foundational national digital identity. Rather, citizens require robust means of digitally *verifying* their identities in trustworthy ways—a subtle difference, that helps avoid accusations of high-modernism while achieving many of the same benefits. And, in public sector contexts, One Login is well-placed to do this. The programme is already years into its development, with much of the required architecture built and nearly four million accounts up and running (Trendall, 2024b). Assuming One Login can continue to ingest an ever-growing range of identity evidence, adequately

proofing identities for those that want them[129], this is an obviously superior solution to a new, centralised identity register.

When it comes to liberty, One Login currently also fares pretty well. Positively, GDS try to offer people two important kinds of choice. First, as mentioned, citizens can create multiple accounts, with different unique identifiers (One Login Support Team, 2024). Though this makes administration less straightforward for civil servants, it does allow people who want to segment their lives to do so, thereby reducing the scope for central, surveillant oversight over their interactions with the public sector. In accordance with my emphasis on digital verification, not identification, policies like this make individuals' lives easier, rather than necessarily making people more legible to officialdom. Instead of mandating a single, reductive identity, One Login dynamically builds-up a picture of the individual, and will one day allow them to draw on evidence from a wide range of different trusted sources—the DVLA, HMPO, GRO, and more. The scheme's power is thus that it can match people's identities across all these datasets. As fraud expert David Black explained, in the context of Verify, this is an often "overlooked" capability in identity systems. With a robust system for verifying identities from existing evidence in place, government can then begin to 'join-up' services for those that want such an offering, and consent to it, without having created a foundational identity database. And, while I suspect that most people are unlikely to worry too much about having a single One Login, the ability to make multiple accounts for those that will is nevertheless worth preserving. It should help to build trust, and so can be expected to further reduce civil society's privacy concerns.

The second kind of choice is over whether or not to use One Login in the first place. It is imperative to retain this optionality. Here, I am wary that GDS's culture of techno-solutionism may need actively resisting. Otherwise the 'choice' to use One Login could be lost if it ever reaches a critical mass. After all, while One Login may improve upon existing systems in many ways, it will remain important to accommodate the ID-challenged as well as the many people without sufficient digital skills in Britain. Collapsing public sector identity provision to One Login alone would therefore be a mistake. Some people may simply never want an account, even if non-digital routes are eventually added. Forcing sign-ups could thus also reignite fears of authoritarianism[130]. Instead, Starmer's government should prioritise reinvesting the money saved by One Login to bolster other, non-digital systems—even if these

[129] As we know, the big problem One Login currently faces is inclusion—which I will turn to in a moment.

[130] As Tom Fisher explained to me, while "it may be that we trust the current government" enough to allow this, adequate safeguards and fallbacks need to be in place in case a new government ever came in with "different priorities" that could undermine freedoms using the systems already in place. He consequently also supported the capacity for "multiple identities even within a single sign-on government system" like One Login.

separate schemes are eventually digitised at the backend. DWP should, for instance, be given more funding for face-to-face Jobcentre checks. Philosophically, the motivation here is classically-liberal—Rawls's (2005, p. 302) stipulation that any inequalities in society should always be to the greatest advantage of the least well-off[131]. Taking this to heart would mean that, where those who can benefit from One Login should certainly do so, this will only be acceptable if it frees-up resources to benefit those that current digital systems leave behind. If digital efficiency savings are not put towards supporting the entire population in this way, overall autonomy will be reduced; and an opportunity to address inequality missed, to boot. Freedom over using the system should therefore be preserved.

The other indispensable benefit that building-out One Login will have is political. Government will retain the power to define who its citizens are—avoiding Verify's outsourcing of this vital state function to private governments—while insulating public services from the vagaries of the marketplace. Beyond the economising arguments I made in the last chapter, considering public opinion can also add something further here. One ex-civil servant who worked on Verify told me how user testing found that "users want something trustable from government", not the private sector, when proving their identities to access public services. This accords with more general polling carried out by Lord Ashcroft (2023), which has revealed just how unpopular privatised public services remain in Britain, despite governments having pushed neoliberal values for the past fourteen years. The evidence shows that, although trust in government as a whole has reached new lows, people on the left and right of the political spectrum still overwhelmingly want government to deliver key services, not companies. And the reasons why are instructive, too (Lord Ashcroft Polls, 2023, p. 19): two-thirds of those polled believed that renationalising water, electricity, energy and the railways would lead to "investing more in services rather than taking out profits", and reaffirm "the principle that important services should belong to the people not private companies." There is clearly strong feeling in the country that some services are too important to outsource, and that doing so results in a lower-quality service.

To me, this makes sense. There is no benefit to a market for market's sake. And the British public have good reason to be wary. Take British Rail or the nation's water supply, which were both privatised during Thatcherite NPM reforms (Bevan, 2023). After just six years of private ownership, the railways were in "catastrophic condition" (Moran, 2003, p. 178). And, since then, they have only further deteriorated; "half of trains in northern England and a third of trains nationally were late" in 2019/20, despite spiralling ticket costs (Shapps & Williams, 2021, p. 13). Privatising water and

[131] Wolff (2024) has recently suggested a moderated version, that inequalities should be to the benefit of all, as a possible driving value for the Labour government. Whichever is chosen, the policy outcome for this issue should be the same.

sewage has been equally disastrous. This made even less sense, though, as privatisation created regional oligopolies with no means for competition. The corporate owners of companies like Thames Water have accordingly extracted tens of billions of pounds in dividends, underinvesting in critical infrastructure while saddling these previously-public assets with crippling debts (The Editorial Board, 2023). Due to these failings, and many more in other sectors, "public ownership" has consequently re-emerged [132] "as a desirable and pragmatic response" among policymakers and the public (Gibbs *et al.*, 2024, p. 157). This helps us see why Verify fared so poorly with citizens. People likely could not understand the neoliberal urge to marketise against a backdrop of systemic privatisation failure. Introducing IdPs that needed to pay shareholders and pursue profits, after all, added needless inefficiencies and costs to processes that can (and I have argued should) have been done by the state—not least because Verify's IdPs primarily relied on government's own data to assure identities.

7.4.2. The Good of Identification?

Re-nationalising governmental digital identity provision therefore seems to make sense. This, though, begs the question: is verifying an identity really akin to running the railways or providing utilities? Recalling Wilson's (2022b) arguments about the standard model reifying digital identities into 'things', we have already touched on how, if identities are goods with some inherent value, then markets for distributing them could well be appropriate. On such a view, the state might then be well-placed to regulate the form and function of identities, much like it does for services like water, gas, electricity, and broadband, while leaving their development, delivery, and maintenance up to the private sector. Indeed, this appears to have been the view underlying early attempts at creating identity federations for government[133]—perhaps unsurprisingly, given the standard model's influence at the time (Fishenden, 2020). But, if this conceptualisation of digital identities is accurate, then Starmer's push to bring other key services back under governmental control, via enterprises like Great British Railways or GB Energy, could be readily extended to identity. It would then be an essentially-political decision as to whether the state should own and run whatever the identity equivalent is to the rolling stock, tracks, or pylons. And a left-wing government might well hold that renationalisation allows for more rational, central planning where neoliberal market logics are poorly-suited. But it is here that

[132] Starmer's government intends to renationalise aspects of the rail network within five years (Austin & Whannel, 2024). And similar calls for action surround Thames Water (Slow, 2023). Jeremy Corbyn's Labour Party even included renationalisation of the water supply as a manifesto commitment (Hendry, 2018).

[133] And, indeed, it echoes claims that "data is the new oil" made by the inventor of Tesco's Clubcard (Arthur, 2013). Identity data would consequently need refining, in our case via the processes of GPG 45, before it had sufficient value to the traded.

the analogy starts to break down; I am not so sure that identities do have any inherent value.

Identities are not physical goods, like trains or units of energy. I am not even sure there is much benefit in possessing an identity in the abstract. As Andrew Hindle put it to me, a digital identity's worth is not "intrinsically in the value of the data"—indeed, the data itself is probably next-to worthless. Rather, an identity's value stems from "the risks that it mitigates, or the compliance that it enables, or the services that it supports". A functioning digital identity system is, therefore, what philosophers call an *instrumental* good. The world is not made better by more digital identities. Much like a train journey or a connection to the grid, such systems are not ends in themselves. They are, rather, means to an end; be it getting to work, boiling a kettle, or proving who somebody is. In fact, how we physically go about achieving these ends seems somewhat irrelevant. This has led some technologists to claim that identity is more akin to something like money (Birch, 2014). After all, banknotes are basically worthless—much like the 1s and 0s of digital identities, or the papers on which physical dossiers are printed. Money's value instead stems from what it signifies to another person or organisation—who might, likewise, need to know who I am. This means that money, like identification, can manifest in paper, digital forms, or even verbal IOUs. The medium does not necessarily matter. What matters is what the information it carries says about the person: that they are solvent, who they are, or what they are eligible for. If a digital identity is just data about a person, asserted to some degree of certainty via computerised means, then that assertion only has value if it means something to someone.

To me, this seems to capture the conceptual importance of identities. It also lends weight to my attempts to see modern, digital systems as an extension of centuries-old identification practices. Of course, doing things digitally may make a service more secure, faster, and able to work remotely. And the medium is not totally unimportant—technologies are not morally neutral (Verbeek, 2011). But the underlying instrumental functionality of the identity evidence does not necessarily differ as a result of its digitalisation. The only real differences are that data can be more easily altered and transferred, and are cheaper to store and copy. This partly explains the gradual trend towards identity's dematerialisation, for instance the Home Office's move to replace physical BRP cards with digital eVisas (Home Office, 2024). Lower costs, more efficiency, and greater flexibility are all desirable traits in administrative contexts. But socially-sorting immigrants remains the Home Office system's purpose. At the same time, if an identity's value is not in the identity itself, but rather what you can do with it, then the link to liberty becomes more evident. If I am right, then what people care about is doing something *with* their identity; not its abstract existence or quality. This is one reason why I am, in principle, supportive of One Login. Without

reducing people to a number in a system[134], it rationalises duplicative schemes across Whitehall, making digital identity verification for the public sector easier and more secure. If the scheme continues in the right direction, it could thus increase individual agency and autonomy, while cutting down on fraud and duplication across government.

However, if digital identities are not intrinsically-valuable, but rather instrumental enablers, then this does change some things. First, it reveals how a focus on distributions alone cannot solve our issues. Inclusion is important, but not because everyone possessing an identity is important. Instead, what identity exclusion prevents people from doing, and what has been made to depend on possessing an adequately-verified identity, is what we should be paying attention to. Thinking about identities in this way reveals the extent to which many liberties in modern Britain have been made contingent upon sufficient identification. Right to Rent, Right to Work, the OSA, and voter ID laws are the prime examples, but they are also symptomatic of a more general erosion of universal services provision in favour of individualised, consumerised services (Needham, 2007). Yet because these changes have been gradual, they are not always conspicuous. And I think this can confuse the debate. One senior civil servant put it to me that, "it's a very small minority of people that, when they think about how they navigate the economy and the identity proofing that comes with that, are worrying about their liberty as they do it. […] It's got to be about ease of use every time." But are ease of use and liberty really so different? The identity-related frictions that have been inserted into normal life are the drag on ease of use—and seem like issues of liberty to me. Where, a century ago, the average Briton would have only encountered the borders as a site of formal identity suspicion, where state-backed identification was required, this experience is now becoming far more widespread.

What I therefore want to emphasise is identity's importance for a person's capacities to act in the world. At the level of ideal theory, we might think of Rawls's 'primary goods'—those rights, freedoms, things that "persons need in their status as free and equal citizens, and as normal and fully cooperating members of society over a complete life" (Rawls, 2020, p. xiii). An argument could easily be made that the ability to adequately identify oneself—including through digital means—could, in modern Britain, have become just such a good[135]. Alternatively, a similar, non-ideal

[134] Of course, some reduction will always be required when abstracting away from the rich, lived experience of human life to categories and attributes in a computerised system (Hicks, 2019). But the question is whether this reduction—i.e. legibility—is the goal in and of itself, or just a byproduct of other attempts to bring some benefit to individual citizens. And the fact One Login allows for multiple accounts also heads this off, to some extent.

[135] Jeroen van den Hoven and Emma Rooksby (2008) have already argued that access to information, including via digital methods, has become a primary good—in particular, an important liberty. This is because adequate access to information is required to carry out one's life plan. And, in much the same way, pursuing one's life plan has increasingly come to require adequate (digital) means to verify oneself.

point could be made with reference to Amartya Sen (1999) and Martha Nussbaum's (2000) capabilities approach (c.f. Masiero & Bailur, 2021). Being able to prove one's identity could well now form part of the essential "functionings" that constitute an individual's "substantive freedom […] to achieve various lifestyles"[136] (Sen, 1999, p. 75). In both cases, the extent to which extensive elements of citizenship and living—voting, welfare, housing, working, taxation, travel, and more—now depend on identification would certainly lend support to such arguments. And, recalling earlier discussions of Windrush and trans people, an additional benefit is that these approaches can more readily account for the importance of identity when it comes to respecting individuals as autonomous persons. The capabilities approach is all about promoting human dignity and flourishing, while Rawls was deeply concerned with ensuring the social bases of self-respect and allowing people to choose their own ends. We can consequently connect identity to a much more positive notion of liberty as well as what we are owed as citizens, rather than a narrowly distributional focus on goods.

7.4.3 The Private Sector

With this in mind, One Login and public services must be seen as just one side of the coin. Much more of life takes place in the wider economy, where we interact with companies and the third sector. And it is here that things become a little more tricky. We must first acknowledge that there is, in principle, no reason why One Login could not be extended to work across private sector cases. After all, it is mostly built from and by commodity services available under the trust framework. Indeed, one senior civil servant at GDS admitted to me that they were "keeping open the prospect of better interoperability between sectors", and fully expected to become "dominant in the market" one day. While this would entirely undermine the trust framework's marketplace for providers, from an instrumental perspective it is not immediately clear that this would be a bad thing. As Louise Maynard-Atem put it, most citizens do seem to want "one key that fits all locks", and do not want to be managing multiple identities with different providers. This was part of Verify's problem. In other words, the neoliberal idea of the *"homo oeconomicus"*, acting rationally in the marketplace, is a fairytale[137] (W Brown, 2015, p. 31). If an identity is a means to an end, then the 'good enough' identity—like the 'good enough' bank account—will satisfice for many. And acknowledging this means that one of the chief benefits of the marketised approach falls away. Options introduce friction and duplication, for little benefit. And IdP choice is not valuable if it does not meaningfully increase capabilities or functionings.

[136] This certainly seems to be the view taken by World Bank's Identification for Development (ID4D) initiative, which has rolled out identity systems across much of the Global South (Beduschi, 2019).

[137] For the same reasons most people do not regularly switch bank accounts (Borgogno & Colangelo, 2020), we should not imagine them constantly changing IdPs.

Consequently, it becomes much harder to justify a neoliberal marketplace for digital identity provision.

Nevertheless, I think it is clear that the trust framework must be retained. One Login should not be allowed to become a trust framework provider, let alone the sole provider. This conviction partly stems from the aforementioned debates around CBDCs, the OSA, DfE/DWP data-sharing, and voter ID, which illustrate the enduring potential for identity-related state overreaches. And, once powers are given up, they are hard to take back. Even if we happened to trust this particular government, then ceding the means for state surveillance and identity-related control of things like digital cash, browsing the internet, children's data, and voting nevertheless seem like risks liberals should not tolerate. Furthermore, if Labour are going to continue expecting things like renting a house or starting a job—not to mention proving your age for gambling, buying knives, or alcohol—to depend on identity checks, then expanding One Login to work across the economy seems particularly undesirable. The state does not need to know the identities of people doing these things, and nor should it be involved in these transactions. Keeping these, and other, sensitive spheres of private life separate from any hint of government oversight should therefore be appealing to any liberal concerned with freedom from the state. Even if you or I might have no qualms about using One Login to access these kinds of services, a large minority of people will be less trusting of a governmental system, no matter how privacy-preserving. And the trust framework's providers can achieve much the same outcomes without creating an all-encompassing state system—much as GDS no doubt believe their solution would be better for users.

Counting against the trust framework, however, is the economisation of identity. But I would argue this is tolerable so long as One Login is not involved. In the market, after all, people are already consumers, so the moral quandary of consumerisation is less acute. Citizens are literally buying services and products, unlike in the public sector, where neoliberal logics have colonised political considerations of liberty, justice, and citizenship (Habermas, 2005). While trust framework providers will thus likely treat individuals' identities somewhat like commodities, evaluated and priced-up according to the risks they pose to a business, this is a lesser concern. While regulating the marketplace for private sector identities—to ensure people can do the things they need to do, with dignity—will be important, the stakes are lower. Monopolisation, exclusion, and the exploitation of people's data are the main outcomes that need to be headed-off to generate an acceptable scheme. But this is precisely the point of the trust framework and its rules[138]. Its specific prohibition

[138] Of course, some providers may well decide not to get certified. But is there really much of a choice around businesses using the trust framework? Given that marketplaces for digital identities have repeatedly failed to take off, there is reason to think that this choice for businesses may be less obvious than it seems. The public dialogue DSIT carried out is instructive here, as citizens were clear that they were looking to government to set standards before adopting digital identity services (DSIT, 2024b).

against using identity and attribute data for third-party marketing is one such requirement that should be praised as positive for privacy and dignity (DCMS, 2022b). But much more can be surely be done if an understanding of digital identities as instrumental, positive goods becomes the scheme's driving force. Careful regulation will, for instance, be needed to avoid swapping state surveillance for corporate. Yet, in principle, there is no reason to think people having multiple identities with different providers is any worse than having numerous bank accounts. And it is hard to see choices of consumer preference over different services as a bad thing[139].

7.5 Towards the Future

I have, thus far, described a state of affairs not too dissimilar to the status quo. I have, however, made clear that both One Login and the trust framework should focus on identity verification, not the creation of new, foundational identities, and that each should remain constrained to their respective sectors. This was primarily for privacy and legibility reasons, as creating a monolithic identity system stretching across the entire economy was likely to dredge up centralisation and surveillance fears. Another upside is that it has also helped avoid the economisation of citizenship, constraining consumerisation to commercial contexts. But an ancillary benefit is that trust framework providers can then provide a buffer between the government and wider economy. This is necessary because there are not many trusted sources for identity evidence. As Kaliya Young put it, "states are the anchors for people's legal- and paperwork-based identity". Most institutions of any importance—banks, airlines, solicitors, etc.—are accordingly unlikely to trust identities built on evidence that does not stem from the state; and, indeed, are often explicitly regulated to this end. Government, then, has an important role to play. It must continue to provide trusted sources of evidence for proofing digital identities, and oversee the ecosystem of providers. But I have been clear that the state should do no more than this in the wider economy. One Login should remain concerned with public sector use cases alone,

---

In other words, citizens say they are unlikely to use uncertified services. This will only be compounded by the fact that accessing government data for the purposes of identity verification will only be possible, as the Bill is currently written, for certified providers (DPDI, 2024). There is therefore reason to think uncertified providers will be disadvantaged and find it struggle to compete, which makes good governance of the trust framework all the more important. This, however, connects to a related issue. In the Bill, DSIT has left scope for, with time, the governance body eventually becoming an industry body (DPDI, 2024)—although the department has committed to staffing the organisation with civil servants and keeping it internal for at least the next few years. Allowing industry to police itself, however, does not strike me as effective, particularly if the trust framework becomes dominant in the wider economy. Preventing corporate capture will thus again be vitally important. And my recommendation would be that government retains its key role in governing the market.

[139] Andrew Bennett, David Black, David Rennie, Joseph Spear and several off-the-record interviewees all put this point to me.

while trust framework providers function as a kind of firewall between government data and private sector RPs.

Under this arrangement, the trust framework will help increase citizens' freedoms, reducing their reliance on outdated and insecure methods of identity verification, without the state gaining inappropriate oversight. In cutting down on paper-based avenues for identity theft and fraud, a significant limiting factor for human flourishing across the economy can thereby be reduced. Yet the challenge is that such a split in power—with two largely-separate spheres of life, governed by two different systems—will require careful balancing. For instance, a stable solution will depend on DSIT continuing with its genuinely open approach to policymaking. Otherwise, government could lose sight of how evolving conditions in the private sector are affecting citizens' freedoms, or could fail to respond to providers' changing needs. And, now that GDS have merged with DSIT, they should ideally adopt a similar approach. More closely involving civil society and other stakeholders can, after all, be expected to help reduce their penchant for high-modernism—going beyond the limited influence of advisory groups (GDS, 2023). But even though my characterisation of the two schemes has thus far cleaved closely to the inherited position, a few, larger changes are needed to ensure that I can arrive at a coherent rationalisation. With these final three suggestions, I will accordingly diverge further from the civil service's current plans. The first is intended to prevent predictive technologies from seeping into governmental identity provision. The second should help address the enduring inclusion issues with both schemes. And the third attempts to purge neoliberal values from both sides of British identity provision—for good.

7.5.1 The Risk of Prediction

My initial point of departure responds to One Login's predictive potentiality. This ambition still drives the programme: GDS have explicitly stated that they want being logged-in to become the "default behaviour" of people browsing GOV.UK, so they can track and algorithmically target users based on their browsing data (Jones, 2022). If a user accesses information about marriage, for instance, One Login will recommend they consider guidance about spousal tax benefits or wills. GDS may even be able to pre-emptively notify users about, or even sign them up to, services or benefits for which they are eligible. This is all intended to make GOV.UK more useful, following in the algorithmic footsteps of the private sector 'Big Tech' giants; Alphabet, Amazon, Meta, Microsoft, and X (previously, Twitter). But it is by no means uncontroversial. Rendering user needs transparent to the state, all tied to a persistent, unique identifier, is key to offering this kind of personalised experience. And pockets of the public are clearly concerned; responses to last year's consultation on the issue were overwhelmingly negative[140]—three-quarters of in-scope responses disagreed

[140] *Vide supra*—discussion of the DEA in footnote 127.

that GDS's predictive system would "improve or target a service to individuals", "provide them with a benefit" or "improve the[ir] well-being" (Cabinet Office, 2023). And only a shockingly-low 2% thought the changes were likely to achieve these goals. People's main worries were "the erosion of data privacy and protection, data security against cyber attacks and a general mistrust in government use of personal data" (Cabinet Office, 2023). And, for most respondents, these risks outweighed any potential upsides.

Whether or not such worries will come to a head remains to be seen. But I think we already know enough to think there may be cause for concern. It is relatively easy to draw from existing research evaluating Big Tech's development of these predictive capabilities. There is much to appraise here, but the short version begins with recognising that, over the past few decades, we have witnessed the 'datafication' of vast swathes of human action and experience (Mayer-Schonberger & Cukier, 2013). During this time, people's actions online have been recast as resources for data-generation (JEH Smith, 2022; Zuboff, 2019). Using Big Data analytics, machine learning, and other artificial intelligence techniques, the dominant technology companies claim to be able to infer our characteristics and interests from the masses of data they collect to build highly detailed user profiles (Couldry & Mejias, 2019). Likewise, though less well-known, companies like Palantir, Cambridge Analytica, and Faculty AI have brought these techniques to bear on politics and the public sector. In both contexts, algorithmic profiling is said to provide meaningful insight into what populations are thinking and feeling, with the promise that these predictions can then be converted into influence, either via 'nudges' or outright coercion (Burr & Cristianini, 2019; Yeung, 2017). Whether or not this is true, global markets have generously rewarded companies with the expertise to solicit, refine and monetise all this data (Flyverbom, 2019, p. 8). And all of this can, at least in principle, be extrapolated to GDS's attempts to build a similar predictive system—raising new normative risks for the programme, beyond those linked to identification alone.

I am certainly wary of these algorithmic technologies being adopted by the state. First, such algorithms have been repeatedly shown to encode bias and discrimination if poorly trained (Noble, 2018; Véliz, 2021). Second, in terms of liberty, there is something deeply uncomfortable about governments profiling citizens to influence behaviour (Sætra, 2019; Yeung, 2018). At the extreme, Western fears about China's attempts to create the 'perfect citizen' via social credit systems provide a useful bogeyman (Orgad & Reijers, 2021). This is straightforward coercion of the kind that few liberals, of even the most positive variety, would countenance. In a liberal democracy, after all, personal autonomy is a "cardinal moral value" (MacKenzie, 2008, p. 512). And seeking to control individual behaviour via surveillance is not easily

reconciled with an appreciation for such autonomy[141]. But if companies carrying out this kind of profiling could weaken democracy and reduce liberty, then governmental attempts should cause far greater alarm. After all, it is one thing for private companies to have this level of insight into our lives, but it would be quite another for the state to employ these techniques, given its monopoly on the use of violence. For one, we can somewhat meaningfully opt-out of interacting with Big Tech's products, but avoiding the state is all-but impossible. One Login, additionally, would not only be profiling us, but taking the further step of tying this information to our formal, legal identities. This will likely make us far more transparent and legible to the state—breaking down the boundaries between our algorithmically-inferred identities and digital identities proper[142] (West, 2019).

At the very least, such a development would take us well beyond the panopticism that identity cards could have realised. The surveillance that can be performed when people are not only formally identified, but their needs and emotions inferred by algorithmic profiling, is uniquely invasive—such systems can, at least in theory, see past what human analysts could to expose subtle patterns and correlations which get at our deeper selves (Cohen, 2012, p. 1919). Yet, on the flip side, the dystopic potential of such systems is not guaranteed. There are also some potentially positive reasons to adopt predictive technologies in government. For instance, Jacob Sparks and Athmeya Jayaram (2022) have suggested that automation could remove arbitrary and discriminatory human decision-making from public services delivery. As they contend, algorithmic systems could actually increase freedom, even equality, by limiting bureaucrats' scope for selective application of the rules. Overall, though, I suggest there remains cause for caution. A future in which a GDS algorithm can make opaque decisions about, say, an individual's welfare payments—based on purported changes to their employment status inferred from their GOV.UK interactions—certainly makes new room for algorithmic upset[143]. And, by removing humans from the decision-making chain, there may well also be less means for recourse. Without the opportunity to argue with a caseworker who can rationalise a decision, citizens could be left facing 'computer says no' answers due to a lack of informational transparency (Bovens & Zouridis, 2002; de Laat, 2018). The risks just do not seem worth it. Consequently my first proposed change would be to nix GDS's predictive ambitions and keep the programme focused on identity verification alone.

---

[141] As philosopher Carisa Véliz (2024c, p. 188) has argued, because autonomy is weakened by algorithmic manipulation of individual behaviour, through the constraint of options, then "so is the democratic ideal."

[142] The Communist Party's genocide of Uighur muslims relies on digital identity systems enhanced by machine learning techniques (Andersen, 2020).

[143] If this seems outlandish, remember that such functions do tend to creep; systems initially limited to one purpose have a habit of expanding into new areas over time, often exceeding the bounds of what we might have accepted with forewarning of the eventual outcome.

7.5.2 Solving for Inclusion

My second alteration would be intended to address the pervasive exclusion problems that both One Login and the trust framework still face. There are multiple ways this could proceed. One approach, as a senior civil servant pointed out to me, begins with recognising "we do not have a right to identity in the UK". Unlike countries with identity cards, the British state currently faces no obligation to provide citizens with means of verifying who they are in the offline world, let alone online. Yet an overwhelming number of my interviewees thought this should change. And, beyond a right to civil registration (Szreter, 2007), the right to a formal, digital identity could certainly be one way to tackle exclusion. As Benjamin Welby argued, "nobody should be denied the ability to get [an identity], which I suppose makes it a right." But, in the absence of a mandatory register, what would delivering such a right mean in Britain? After all, state systems like One Login and Government Gateway are already freely available to any citizens with adequate identity evidence. And all currently-certified trust framework providers pursue a 'free at the point of service' model. Even if the market did start charging people to use their identities, what would a new right change? Perhaps a solution could involve government operating as what Nick Mothershaw calls a "provider of last resort" under the trust framework. In other words, the state would guarantee services to those people it is otherwise uneconomical for businesses to service—supporting those whose identities are more difficult to proof.

Many interviewees thought some variation of this concept would help, and that government should play such a role. Guy Herbert, for instance, contended that a right to digital identity was "nonsensical except in the sense that there ought to be an official agency or quango charged with doing that, perhaps semi-detached from government". Yet I do not think this is a desirable outcome. One obvious drawback is that it would entirely undermine the trust framework's fledgling marketplace—governmental identity provision would make a mockery of market pricing. As Adam Cooper noted, "You can't really compete with government; they're always going to have a better chance of getting things done, because they can either legislate you out of competition or they can outspend you." Providers currently charge RPs when verifying an identity to a particular level, and although government could likewise levy a price from RPs when providing a 'last resort' service, this would evidently skew the market—not least as government would not necessarily need to make much, if any, profit. Add to this that government would be regulating an industry it was participating in, and it is hard to see how a fair and stable market would develop. This was Nick Mothershaw's main concern. But I think a larger concern is that this would, by the backdoor, also bring back just the sort of governmental oversight I have already ruled out. Not only this, but that oversight would only be affecting the already-disadvantaged, simultaneously bringing back the potential of service discrimination based on

provider[144]—while such groups are already more likely to be subjected to surveillance, data misuse, and other privacy invasions in the first place (Véliz, 2024a, p. 194).

All this aside, we must acknowledge a more fundamental point: that neither establishing a provider of last resort nor giving people the right to an identity actually solves the underlying issue. The problem, in reality, is that both One Login and the trust framework largely rely on photo IDs. The true bottleneck is consequently GPG 45—the guidance which underpins the programmes. And, while a variety of evidence can be accepted under GPG 45, achieving higher levels of confidence generally requires a passport, driver's licence, BRP, or equivalent international documents (DSIT, 2024a). However, as we know, a corollary of this is the necessary exclusion of those who cannot afford or do not otherwise possess such photo IDs. And this is not simply solved by mandating a right to an identity, nor delivering identity services via the public sector. Thus far, the only fixes we have discussed involved data-sharing and greater access to government data. For trust framework providers, as discussed, powers in Labour's Digital Information and Smart Data Bill could theoretically help boost inclusion, one day, by getting additional identity and attribute data out of government. And we know GDS are pursuing a similar solution under the Digital Economy Act 2017. But both of these data-based fixes are, as mentioned, promissory. The technical architectures needed have not been built, with most departments still stuck with systems in need of modernisation before such data could be shared and utilised for identity proofing. I am therefore not convinced this option is sufficient—though it should still be pursued in case it can one day help deliver better inclusion outcomes.

In the meantime, a more effective fix is readily available. And, rather than numerous departments needing to build out novel digital identity and attribute infrastructure, taking on novel liability for data they would be newly sharing, it would instead involve departments that are used to handling identity evidence simply enhancing their existing capacities. In the short-term, this feels far more realistic. I see two possible avenues. First, equipping DVLA with the capacity, which they have long trailed, of issuing mobile driver's licences (mDLs) (DVLA, 2021)—essentially, digitised versions of normal licences—and, more unusually, then liberally distributing these to any citizen who wants one, for free. Many countries, like America, have already gone down a similar route, issuing physical 'non-driver's driving licences' to people who lack identity evidence to get them through the door (c.f. AAMVA, 2020). The reasoning here is that, if maintaining GPG 45's robust standards requires photo IDs, then why not just issue more photo IDs? Of course, this would not be hugely dissimilar to people applying for provisional licences when they have no intention of learning to drive. The difference is that the associated cost would need to be removed, and the provisional scheme would need to be extended to any individual

[144] This, as you will recall, was David Rennie's concern with a hub-less design for Verify.

that wanted access. Yes, DVLA would need additional funding and support to handle such an expansion, but this would no doubt be easier and cheaper than equipping multiple departments, like DfE or the NHS, with whole new digital identity credentialing capacities.

The only drawback, according to one senior civil servant, is that DVLA's proofing processes are not the most rigorous. Consequently, I think a better option could actually be for HMPO to freely issue people with some kind of digital travel credential. While no process is foolproof, HMPO's is certainly more rigorous than DVLA's, which is why this would be preferred[145]. HMPO also already support inclusion-friendly methods such as social vouching to get people without sufficient documentation access to passports (HMPO, 2024). And there would be no associated risk of people travelling illegally—the digital passport could be constructed in such a way that it could record who had permission to travel, and would update in realtime. With either of these options, however, utilising the identity binding infrastructure already provided by One Login would allow this novel digital evidence to readily form the basis for identity verification processes that are more robust than the paper-based checks we currently rely on. With GDS helping ensure that the correct credential was bound to the rightful owner's digital identifier, this data could then be released from government and used to help verify identities across the public and private sectors. And, as international standards for both mDLs and digital travel credentials have already been developed, this route would be relatively cheap and straightforward to implement when compared with many of the other options for increasing the population coverage. As one civil servant working on identity agreed with me, "it is going to be more cost-effective to help [people] get a passport or a driving license and then use that to create digital identity."

The risk here is that the appropriateness problem could reemerge. Passports and driver's licences are not, as we know, designed as identification documents per se, so should not be used as such in the wider economy if it can be helped. But this solution sidesteps that problem, retaining digital credentials as mere evidence for an identity, rather than identification itself. The actual digital identities individuals would be equipped with would be created under either One Login or the trust framework using this evidence—replete with all the anti-fraud and identity verification measures built into both schemes. The resulting identities would accordingly be proofed to a far higher standard than those generated by most existing systems, while benefitting from far better inclusion outcomes. A relatively minor investment from government in providing free mDLs and/or digital passports could thereby open the door to a far more equitable system—addressing the inclusion problem at its root. And, as a result,

[145] David Black told me it is possible for some fraudsters to "spoof you enough to be able to go to […] get a passport issued in your name." Fraudulently obtained genuine documents do exist. But HMPO's systems are more rigorous than DVLA's.

this solution would open up the benefits of digital identity provision to far more people. The ability to do things digitally, across the entirety of the economy, would thereby be extended—while those who, for whatever reason, did not feel comfortable or able to do so would face no obligation to take part. I think this genuinely represents the best of all worlds in terms of a realistic compromise, oriented towards maximising liberty and inclusion within the realms of the possible. It accordingly represents Labour's best chance of finally meeting Chango's (2022) terms and properly digitising identity provision in Britain.

7.5.3 Identity Under Labour

This brings us to my final suggested revision—a response to the remaining, albeit much-lessened, economisation of citizens' identities that remains under the trust framework. While the changes I have already proposed would move us away from the Conservative's neoliberal reimagining of the consumer-citizen, some degree of consumerisation in the wider economy would persist under current proposals. Now, it may be that this is not a pressing concern. Free enterprise and participation in a market-based economy have long been staples of British liberalism. And I certainly think that providers who meet the trust framework's rules on a for-profit model should be welcome to continue offering their services. But encouraging one final change to the landscape could take us towards a more Labour-coded outcome. The idea would go something like this. Rather than a marketplace of competing providers, the trust framework should be better conceived of as an ecosystem of different services operating under different funding models. Some may well operate for profit, but I think that others could—and perhaps the majority should—operate instead under the co-operative model. This essentially extends the case Dan Hind (2019, p. 24) has made for a 'British Digital Cooperative', which would "be established by Parliament as a public cooperative whose members are the citizens and residents of the United Kingdom", managed "jointly by its workforce and by the public". Rather than the trust framework advancing industry's values, the idea is essentially to replace these with the people's values, as served by a new kind of identity provider—or even multiple such providers. After decades of neoliberal, top-down central planning, not to mention marketisation, why not let the people have more of say about their identities and how they are managed?

Co-operatives have a long history, and are essentially British. They have their roots in the working-class labour movement of the nineteenth century, where their primary function was not to make money, but rather to "promote and serve the interests of […] members" at a time of economic hardship (Robertson, 2016, p. 1). Although originally focused around communities working together to exchange, source, and sell "basic provisions", the movement soon expanded, and "developed collective resources to meet a range of social and economic needs" (J Wilson *et al.*, 2013, p. 274). Through collaboration, co-operatives sought to equip their members with something like a basket of primary goods, or the materials and support needed to

realise their capabilities, anchored in ideas of the community and reciprocity—each member was a stakeholder is the good of the community. Even today, the Co-operative Group provides banking, insurance, funeral care, mobile phone packages and, of course, food and drink—as well as distributing a yearly dividend to all members, splitting a portion of the group's profits (Co-Operative Group, 2010). The model's utility for tying adequate identification to the promotion of positive liberty should thus be evident. And, as mentioned, Hind has already proposed a more general co-operative for the digital realm, envisaging a competitor to Big Tech operating under the model. The intellectual resources are therefore ready and waiting to be transposed to digital identity. The result would be new identity providers, premised upon democratic participation and oriented towards meeting citizens' and residents' identity-related needs—without profit as the primary goal.

Consequently, this final proposal could offer a way to satisfy the views professed in the Lord Ashcroft polls, without nationalising British identity providers[146]. Services in the private sector could remain privatised, but would, at the same time, now need to compete with an alternative that belonged to the people—offering a novel way to crowd the market out of an area of life that has become centrally important to exercising liberty and flourishing in twenty-first century Britain. Perhaps this would end up merely replicating other regulated markets, much like what we today see in, say, banking or the utilities sector. After all, the Co-Operative Group already competes with for-profit providers in both these spaces. But pursuing such non-commercial solutions, Wolff contends, has the twin benefits of not only making "a normal range of fulfillments available to a broader range of people", who might not otherwise be able to afford them (Wolff, 2011, p. 185), but, additionally, can promote greater social solidarity, thereby reducing the desire to ask questions like 'what's in this for me?' that can so damage the public sector (Wolff, 2011, p. 189). For liberals, this proposal would thus push us towards a more egalitarian understanding of individual identity needs, while also shoring-up a non-commercial version of citizenship. And all of this would be achieved under a model of collective enterprise that promotes the betterment of society and the needs of stakeholders, not shareholders (Borkin, 2019). For Starmer's Labour Party, the opportunity to fertilise a uniquely-British take on digital identity provision—with a five-year runway to seed this new business model, start issuing digital credentials to solve for inclusion, and scrub predictive ambitions from One Login's roadmap—should accordingly be considered.

[146] This also links to recent attempts to flesh out a kind of digital public infrastructure (c.f. Zuckerman, 2020), and would build on the popular notion of identity as the "missing layer" of the internet (Cameron, 2005).

Chapter 8.

Concluding Remarks

> "[T]he move to computerize and digitize means that many preexisting cultural forms have suddenly gone liquid, losing their former shape as they are retailored for computerized expression. As new patterns solidify, both useful artifacts and the texture of human relations that surrounds them are often much different from what existed previously"
>
> *– Langdon Winner (1997)*

This thesis has argued that a liberal-theoretical perspective can help resolve the interlinked normative concerns that have, for decades, clouded national digital identity policy in Britain. These closing remarks summarise my contributions, present some reflections on the project and its limitations, as well as suggest avenues for future research.

As you will recall, we began with the recognition that we are in the midst of an identity revolution, driven by monumental changes around how we communicate and interact. In just three short decades, internet use has exploded, connecting the world and enabling new forms of social and economic cooperation (EA Whitley & Hosein, 2010, p. 3). The internet, though, was not built with identification in mind (Cameron, 2005). The assemblage of paper documents and processes that previously sufficed has therefore struggled in a world of remote exchanges. Rates of fraud and identity theft have soared, while normal people have struggled to keep up. What is worse, people who were already excluded have been left to fall further behind. But we also uncovered deeper concerns, underlying these more practical issues, to do with the nature of the state and its relationship to modern citizens.

In light of Britain's unique struggles with identification, I have therefore constructed a novel, liberal framework to diagnose these issues—the first such rationalisation of historical identity systems in political-philosophical terms. With this in hand, I then evaluated contemporary schemes and, ultimately, justified a series of changes to One Login, the trust framework, and the provision of digital credentials that would, I argued, together facilitate a more coherent way forward.

8.1 Findings and Recommendations

Following the scene setting of *PART I*, each subsequent chapter of this thesis has detailed one era of digital identification policy, and usually one identity system. The exception is *Chapter 4*, which was wider in scope. Here, we evaluated how the British state increasingly interfered with people's liberties over the course of the twentieth century. As nation-states defined themselves on the global stage, Britain exerted newfound control at home—particularly at the borders—and showed it was not afraid to use analogue identification systems to filter, socially sort, and discriminate. Using techniques refined abroad, British subjects were made centrally legible for the first time. At times of 'total warfare', such interferences were begrudgingly tolerated (Higgs, 2011, p. 119). But, following the conclusion of each World War, central identification was swiftly rejected—even though some of the associated changes for public administration would live on.

Sweetening the deal, however, the social contract was also reimagined, bringing universal healthcare and social security to millions. And any reduction in negative liberty was more than justified by the increase in living conditions and equality that followed, much to the annoyance of some libertarians. As subjects became citizens, a more positive version of liberty therefore came to the fore. Focusing on particular technologies—seals, papers, or computers—would not have revealed the inherently political impacts of these changes. It was liberal theory that helped highlight how identity systems were used by the state to 'know' and manage Britain's populations.

In *Chapter 5*, we then jumped forward to the early 2000s, and Britain's first national digital identity system. New Labour's identity cards, backed by the NIR, elevated many of the historical issues we had already covered to new heights. Most concerningly of all, digitalisation could have enabled near real-time surveillance of when and how people used their identities; a level of state insight that, despite a growing narrative of securitisation, ultimately proved unacceptable. Although identity cards could have made identifying, policing, and sorting the population easier (Barnard-Wills, 2012, p. 134), New Labour's proposed changes to the social contract were accordingly rejected. Opposition messaging around the 'nanny state' cut through. While immigrants and residents would thus retain BRPs—and, in doing so, become the only population in Britain with a foundational digital identity—British nationals missed out on a solution that might have headed-off the inclusion issues to come. But this chapter also reiterated that digitalisation is not necessary for unacceptable state discrimination; as Windrush's hostile tracking, democratic exclusion, even deportation of legitimate citizens showed. As Rose (1999) had identified years earlier, being able to demonstrate a legitimate identity had already been made essential to exercising liberty and enjoying the full fruits of citizenship. The modern state has therefore put the onus on citizens to prove who they are, and what rights they have, even while it has failed to provide them with the means to do so.

As this demonstrated, government still urgently needs secure ways to remotely identify people. And, as more public services move online, the local, face-to-face interactions that historically sufficed have become increasingly insufficient. *Chapter 6* accordingly explored the promise of federating national identity. Contra identity cards, where government had asserted itself as sole arbiter of formal identity, Verify gave citizens a radical series of choices over their digital identity provision, much like consumers in a marketplace, in collaboration with the private sector. Identity was thus made just one more product amongst many. In doing so, this development highlighted the limitations of a division between the public and private sectors that liberals and surveillance/service state thinkers have traditionally respected. Of course, Verify also failed to address the inclusion issues of existing forms of identification, thereby replicating these issues digitally. But the primary normative concern I raised was how the programme imported neoliberal market logics to political considerations of citizenship and access to public services. As I argued, although the scheme was meant to increase liberty, giving users choices, it actually saddled citizens with a much-impoverished understanding of freedom—reducing them to commercial, not political, actors. I accordingly rejected the privatisation of the citizen-state relationship and its intermediation by corporations, as the political dimensions of state identity were being neglected.

In *Chapter 7*, we then finally turned our attention to the systems of today. I suggested that the civil service appears to have learnt important lessons, though warned that GDS's techno-solutionism may persist. More positively, I praised One Login for jettisoning the consumerisation of governmental identity provision, and placing inclusion high-up on the agenda—even if it remains unresolved, for now. And, while the trust framework retains some of Verify's problematic aspects, and suffers from the same fundamental inclusion issues as One Login, I nevertheless argued that the scheme was also worth keeping. Reasserting a public/private split has certainly helped.

With key normative concerns identified in prior chapters, though, it was relatively straightforward to propose sensible revisions to modern systems, tackling each issue in turn. An important first step was ruling out the conflation of digital and algorithmic identities. I then proposed an answer to the inclusion problem involving the free distribution of digitised credentials to those who lack sufficient identity evidence. Whether it is HMPO or DVLA that takes up this mantle, this is one of the only ways I could see to square the circle and avoid introducing another monolithic centralised digital identity. Finally, I contended that promoting a co-operative model under the trust framework could further limit remaining consumerisation concerns, while ensuring citizens gain more of a say over who maintains their identities in a characteristically Labour-coded way. Though we have not therefore ended up too far from the inherited situation, these changes still add-up to a coherent, feasible solution that improves upon the status quo.

8.1.1 Reflections and Limitations

I began this thesis with a story about a demonstration in Oxford. While I doubt many of the protestors mentioned at the outset would approve of my proposals, I nonetheless stand by these recommendations for several reasons. First, I have aimed to outline a realistic solution, one that iterates on the hand government has been dealt, without rejecting digital identity systems outright. It is clear that such systems carry many benefits, and are the increasingly-necessary foundation of the digital state. While I am therefore saddened by the gradual displacement of interpersonal, social relationships by administrative systems, I also accept that it is likely too late to return to a Goffmanian utopia. The internet, and digital identities, are here to stay—and our existing, analogue systems are evidently failing us. Second, and relatedly, I have been highly critical of different digital identity systems' various negative effects, and sought to outline solutions wherever possible. I have argued that central oversight, unjustified exclusion, and the economisation of the citizen-state relationship are all particularly unacceptable. While I do countenance identity systems, I have thus made sure to emphasise that these downsides must be addressed for a solution to be suitable on a liberal basis. Finally, my novel conceptualisation of identities as a kind of instrumental liberty—empowering people to realise valuable ends, and a necessary part of modern life—should provide an important yardstick for judging any future developments[147]. While any equilibrium can be fleeting, liberals will always value freedom; and this should help point the way forwards, whatever comes next.

As I will elaborate shortly, filling these gaps and making these recommendations has only been possible due to my utilisation of an empirically-informed flavour of reflective equilibrium. I think this is evident from the evolution in my thinking from the earliest years of this project. Comparing where *Chapter 7* ends up to the initial position I outlined in *Chapter 1*, it is amazing how alien my foundational beliefs in 2019 now seem to me. Most notably, my faith in parts of government to deliver an effective system has been thoroughly shaken; though I do think DSIT's open-policymaking approach provides reason for hope, if corporate views can continue to be tempered by a concern for society at large. The sheer moral and political complexity of the issues involved—the meaning of identification for liberty, the rampant exclusion that existing systems perpetuate, and the inappropriate privatisation of public identity services—have shown me my prior naivety. Although a mandatory identity card system could theoretically solve these issues, I now see how a century of cultural contestation makes alternative solutions far more desirable.

But, without strong Ministerial support and direction, I do still fear that aspects of contemporary identity policy could remain tarred by the techno-solutionism and

[147] Along these lines, I agree with Simon Szreter (2007, p. p81) that "Identity registration systems must be created principally for the liberty and the use of private individuals, and not to serve the purposes of commercial organizations or states".

high-modernist tendencies of the state. One Login is certainly at risk of this. And, without a concerted effort to fix inclusion, twenty-five years of failure to get either a centralised system or federated marketplaces off the ground could continue to define British identity policy. The neoliberal promotion of marketplaces for their own sake must therefore be ended, and focus put back on ensuring that citizens and residents can actually *do* things—exercising a fuller kind of freedom—thanks to a functional system.

Without the fifty-one interviews I conducted, I would never have been able to develop anything like a holistically-informed understanding of the problem space. I am therefore deeply indebted to my participants for all their time and expertise. But there are always limits to what is possible. First, most of my fieldwork was completed just over halfway through this project, by mid-2022. And while those conversations had significant import, being able to conduct follow-ups in light of the changing political context would have been one useful way to build an even more coherent and robust equilibrium. Especially in light of the election, I wonder if the viable options may have shifted, and whether this might have altered some of my discussions—particularly with civil servants. Election aside, my own views also developed over the project, and being able to revisit conversations once I had learned more would have been hugely beneficial. Of course, practical limits on my time and funding meant I missed out on many conversations that would no doubt have altered the final outcome. I hope to speak to many more people down the line. Finally, it is also worth reiterating that I only spoke to elites and experts in the identity space. While some of these people were incidental users of the systems discussed, emulating Wolff and de-Shalit's (2007; 2024) focus on talking to 'normal' people would no doubt have raised additional, different considerations. Although I do discuss this in *Chapter 3*, it remains a possibility to explore in the future[148].

On the topic of methods, it is worth saying just a few more words about reflective equilibrium. Elsewhere, I have argued that the method requires a twenty-first century update if it is to remain relevant and achieve widespread actual usage (CH Smith, 2023). In the paper, I contend that certain digital tools provide us with better ways to construct and share equilibria, taking seriously the inherent reproducibility of digital data. In short, I urged theorists to begin publishing their *digital reflective equilibria* (DRE) in their entirety, online, so that others could explore this justificatory content accompanying their work themselves. I originally thought I could at least attempt to demonstrate the value of constructing DRE in this project. While fully realising these proposals would have required cooperation from journal publishers or the

[148] One particularly interesting area to explore would be biometrics, which seem to have become far more acceptable, despite the traditional historical aversion to such technologies and techniques in Britain (see Chapter 4). Understanding what has changed—whether it is features like TouchID and FaceID on Apple Products, the rise of cameras in our pockets, or something else—by discussing these issues with everyday users would be fascinating.

University's research archive, and so were far beyond the scope of this thesis, I did anticipate being able to publish something like a digital map of the final equilibrium I constructed for this project alongside the text of the thesis itself. Evidently, this was not possible in the end. One expected methodological contribution I initially expected to make—demonstrating the value in DRE with a practical example—was therefore not achieved[149].

8.2 Future Research

A thesis is, in part, an exercise in deciding what not to talk about. Over all my interviews and readings, I have stumbled across many avenues that could not be fully explored. Some of these would make fine extensions to the foundations I have established here. In closing, allow me to therefore note a few of the most promising topics. The first relates to a development we have already discussed at length—that, as one pressure group has argued, digital identification relies on "complex systems that can alter the relationship between the individual, the state, and all the companies and agencies who are granted power in between" (Privacy International, 2020). I am therefore pleased that I have been able to add some theoretical meat to the bones here, linking digital identity systems to liberal arguments around the issues with privatisation. I think the growing role of the private sector could do with more sustained research, however. It is somewhat necessary, in political philosophy, to reify the state. But, following Anderson's (2017) lead, the assemblage of private and public actors that increasingly add up to 'the state' needs careful consideration. As firms potentially gain power and insight through digital identity systems, impetus emerges for considering how IdPs' monetisation of this position might affect society at large. While Big Tech has stolen the limelight recently, these much less-studied providers are coming to manage an equally, if not more, sensitive package of data—and would therefore be an interesting avenue for further research.

In addition to companies lessening the role of the state, we must also consider the prospect of identities unbounded by the confines of the nation (c.f. Kakabadse *et al.*, 2009). What would it mean to use my British digital identity to prove my age in America, or to buy a house in China? International interoperability is frequently touted by government as a possible advantage of the trust framework (DCMS, 2023). But, given the problems the standard model faces even within a country, how would

[149] Although I did not manage to reconstruct a final DRE in time for submission, much of the work I undertook for this project did follow the steps I outlined in (CH Smith, 2023). With sufficient time, a reconstruction would therefore not be hard to complete. More generally, using digital tools to collate judgements and principles from the literature, shape these into a developing whole, and then balance these against views from my interviews, did prove to be eminently achievable. Many of the normative insights made here only emerged through the coding process, which helped me find common threads running through different interviewees' arguments. The DRE method consequently stands ready to be tested and built upon.

these scale to an international context? While people, like states, are physically bounded, the internet is not—and so the dematerialisation of identity that we have discussed raises some unique issues.

Additionally, while I have repeatedly said technology is not the most important consideration in identity, I do acknowledge that technical developments have import for both current systems and future research. On this point, it is worth noting that several of my interviewees outright rejected both centralised *and* federated architectures. One unusually-normative approach I considered but did not ultimately discuss here was so-called 'self-sovereign identity' (SSI) (Mattei *et al.*, 2024). Several of the experts I spoke to are influential in this space, and we explored the potential for decentralisation as an additional architectural option. During the course of the project, the related concept of verifiable credentials has likewise caught on (Sedlmeir *et al.*, 2021), in Europe but also with GDS. Nevertheless, I have not discussed SSI in this thesis, though it is supported by the trust framework, as the approach seems to undervalue the importance of institutional relationships in much the same way as Cameron's federated model[150]. With organs of the state remaining the most important identity institutions for the foreseeable future, providing almost all of the valuable identity evidence, it simply did not seem worth considering yet—without a substantial change in philosophy from government.

The final road I wish to flag as worth exploring is theoretical. At this project's outset, I did not actually think I would be advancing a liberal argument, but rather a neo-republican one[151]. The difference is nevertheless worth discussing. Republicans are "broadly speaking progressive and liberal", though they diverge from liberals in a few key ways (Lovett, 2018). Most importantly, republicans believe that negative freedom—freedom as non-interference—fails to capture the essence of freedom. They

[150] To this end, one of the lessons I have taken away is that the standard model fails to recognise the enormity of the challenge identity poses to important institutions, and especially the state. IdPs, as imagined by Cameron, seem unable to deliver on their promises in many of the most vital contexts. Identity rather appears to be in the eye of the RP, which must be satisfied that enough is known about a data subject for it to manage the risks of interacting with them. 'Adequate identification' is therefore not the sort of good or service that can be easily provided without significant levels of trust or contracting between IdPs and RPs; it is, rather, a state that is defined by the RPs themselves, and so not easily outsourced. The metaphor of reusable identity provision is consequently all wrong; companies distributing 'a' canonical digital identity to each of us makes little sense without a foundational state identity to build upon. Any RP facing real risks, like a bank, would therefore want to know so much about the proofing and verification processes that had been pursed, and have an audit trail, that it would somewhat defeat the point of outsourcing. This is especially true for government. Why should the state trust that a company says somebody is who they say they are? As I have suggested, "simply and safely" being able to "move verifiably true copies of important data around" seems far more realistic as a model (S Wilson, 2022a). Hence, my focus on digitised credentials.

[151] This has nothing to do with the American political party of a similar name which, in its current form, certainly does not espouse the values of neo-republicanism.

consequently reconceptualise liberty in terms of freedom from "domination" (Pettit, 1997, p. 31; Skinner, 2008, p. 90). In this sense, it is an individual or group's arbitrary capacity for interference in the life of another that has truly deleterious effects for their liberty—paradigmatically illustrated by the master-slave relationship (Pettit, 1997, p. 22). In such situations, the mere possibility of domination, even if unrealised, effectively constrains those with less power. Neo-republicans have accordingly linked this insight to critiques of state mass surveillance[152] (Hoye & Monaghan, 2018, p. 349). And I suspect that other digital governmental systems, including identity solutions, might raise similar concerns, given republicans' attention to structural and systemic forms of power and domination.

Allow me to elaborate. At a state level, neo-republicans put in place constitutional guarantees that individuals will be protected from both public and private domination (PT Smith, 2020, p. 50). Citizens must be treated with equal respect and have space to exercise their freedoms. If digital identity systems increase the potential of any group (governmental or otherwise) for arbitrary domination over others, then this would only ever be justified for republicans if that power can be suitably and democratically controlled. China's social credit system, for instance, would not be justified, whilst Estonia's far more transparent digital identity system might fare better. But republicanism is also pragmatic: where a citizen has consented to outside interference (e.g. institutions like the courts), it poses no threat to their freedom (Casassas & De Wispelaere, 2016, p. 285). If citizens decided that digital identity systems served the common good, then republicans could comfortably accept the (suitably-bounded) interference that increased identification might pose. Republicans would simply demand that such systems support the equal participation of all in a society, asking who is deemed worthy of political inclusion and respect. Similarly, because many modern republicans reject neoliberal free market "ideology", and see markets as tools for domination, the notion of a marketplace for identities would be treated with extreme scepticism from the off (Casassas & De Wispelaere, 2016, p. 286).

While liberalism can ground similar critiques, I am minded that the tools offered by neo-republicans could have left less space in the first place for many of the issues we have seen plague identity systems in Britain. Verify, as we know, consistently failed the poorest in society, limiting access to the very benefits that form the 'economic floor' of a republican society (Casassas & De Wispelaere, 2016). And a marketplace model would have likewise been ruled-out almost immediately. In line with the more positive version of liberty I outlined in the last chapter, then, republican freedom seems to capture something about how to tame the unblinking eyes of pervasive digital systems—and ensure they are put towards the common good rather than the needs of the state or corporations alone. While the literature is still young,

[152] Imagine a slave invited to speak 'freely' in the Roman forum. Evidently, their master's presence would effectively limit them, whether or not they were actually interfered with.

and republican attention to the digital dimensions of statehood particularly fledgling (c.f. Susskind, 2022), I do think there is much to draw on here that would add value to a normative critique of identity systems. While Britain is not a republican nation, so the approach would have been less suited to this context, a neo-republican analysis would still be a fascinating extension or complement to the liberal rationalisation I have put forward here.

Regardless, digital identification looks set to remain a 'live' political issue. And, until it is resolved, I hope more academic attention—from numerous perspectives—can continue to help widen my reflective equilibrium, and thereby inform the small role I now play in setting British digital identity policy. I certainly still have much to learn.

References

AAMVA. (2020). American Association of Motor Vehicle Administrators – DL/ID Card Design Standard (2020). Retrieved September 7, 2024, from https://www.aamva.org/assets/best-practices,-guides,-standards,-manuals,-whitepapers/aamva-dl-id-card-design-standard-(2020)

Ada Lovelace Institute. (2021). *What place should COVID-19 vaccine passports have in society? Rapid Expert Deliberation*. Ada Lovelace Institute.

Addison, P. (1994). *The road to 1945: British politics and the Second World War* (Rev. ed). London: Pimlico.

Agar, J. (2001). Modern Horrors: British Identity and Identity Cards. In J. Caplan & J. Torpey (Eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton, NJ: Princeton University Press.

Agar, J. (2005, November 4). Identity Cards in Britain: Past Experience and Policy Implications. Retrieved May 26, 2024, from https://www.historyandpolicy.org/policy-papers/papers/identity-cards-in-britain-past-experience-and-policy-implications

Allum, J. (2020, September 22). Introducing GOV.UK Accounts. Retrieved October 21, 2020, from https://gds.blog.gov.uk/2020/09/22/introducing-gov-uk-accounts/

Alpár, G, & Jacobs, BPF. (2013). Credential Design in Attribute-Based Identity Management. In R. Leenes & E. Kosta (Eds.), *Bridging distances in technology and regulation* (pp. 189–204). Oisterwijk, The Netherlands: Wolf Legal Publishers.

Amoore, L. (2008). Governing By Identity. In C. J. Bennett & D. Lyon (Eds.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (pp. 21–36). London: Routledge.

Amoore, L. (2011). Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society*, *28*(6), 24–43. https://doi.org/10.1177/0263276411417430

Amoore, L, & Piotukh, V (Eds.). (2016). *Algorithmic Life: Calculative Devices in the Age of Big Data*. London: Routledge. https://doi.org/10.4324/9781315723242

Anand, N, & Brass, I. (2021). Responsible innovation for digital identity systems. *Data & Policy*, *3*. https://doi.org/gnttrj

Andersen, R. (2020). The Panopticon Is Already Here. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

Anderson, E. (2017). *Private Government*. Princeton University Press. Retrieved from https://press.princeton.edu/books/hardcover/9780691176512/private-government

Andrews, B. (2022, June 16). How we are improving inclusion for digital identity in government – Government Digital Service. Retrieved March 31, 2024, from

https://gds.blog.gov.uk/2022/06/16/how-we-are-improving-inclusion-for-digital-identity-in-government/

Arendt, H. (2006). *Eichmann in Jerusalem: A report on the banality of evil*. Penguin Books.

Arthur, C. (2013, August 23). Tech giants may be huge, but nothing matches big data. *The Guardian: Technology*. Retrieved from https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

ARTICLE 19. (2022, April 25). UK: Online Safety Bill is a serious threat to human rights online. Retrieved September 10, 2024, from https://www.article19.org/resources/uk-online-safety-bill-serious-threat-to-human-rights-online/

Austin, K, & Whannel, K. (2024, April 24). Labour pledges to renationalise most rail services within five years. *BBC News: UK Politics*. Retrieved from https://www.bbc.com/news/uk-politics-68889345

Avoine, G, Beaujeant, A, Hernandez-Castro, J, Demay, L, & Teuwen, P. (2016). A Survey of Security and Privacy Issues in ePassport Protocols. *ACM Comput. Surv.*, *48*(3), 47:1–47:37. https://doi.org/10.1145/2825026

Baderin, A. (2017). Reflective Equilibrium: Individual or Public? *Social Theory and Practice*, *43*(1), 1–28. https://doi.org/f3s8gx

Baran, PA, & Sweezy, PM. (1966). *Monopoly Capitalism: An essay on the American economic and social order*. New York, NY: Monthly Review Press.

Barassi, V. (2019). Datafied Citizens in the Age of Coerced Digital Participation. *Sociological Research Online*, *24*(3), 414–429. https://doi.org/ggr35s

Barnard, B. (2020). *Verified: The UK's Digital Identity Dilemmas*. Policy Exchange. Retrieved from https://policyexchange.org.uk/wp-content/uploads/Verified.pdf

Barnard-Wills, D. (2012). *Surveillance and identity: Discourse, subjectivity and the state*. Ashgate.

Barnard-Wills, D, & Ashenden, D. (2010). Public sector engagement with online identity management. *Identity in the Information Society*, *3*(3), 657–674. https://doi.org/10.1007/s12394-010-0079-2

Barry, L. (2020). The rationality of the digital governmentality. *Journal for Cultural Research*, *23*(4), 1–16. https://doi.org/10.1080/14797585.2020.1714878

Bauböck, R. (2008). Normative political theory and empirical research. In D. Della Porta & M. Keating (Eds.), *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective* (pp. 40–60). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511801938.004

Bauböck, R (Ed.). (2018). *Debating Transformations of National Citizenship*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-92719-0

Bauman, Z. (2004). *Identity: Coversations With Benedetto Vecchi: 4* (1st edition). Polity.

Bauman, Z, & Lyon, D. (2013). *Liquid Surveillance: A Conversation*. John Wiley & Sons. Retrieved from https://books.google.com?id=flpuJFmDFQYC

Baumberger, C, & Brun, G. (2021). Reflective equilibrium and understanding. *Synthese*, *198*, 7923–7947. https://doi.org/ggkp4w

BBC. (2005, May 25). Blair defends identity card plan. Retrieved from http://news.bbc.co.uk/1/hi/uk_politics/4577087.stm

BBC. (2009, November 16). ID cards 'good for going to bars'. Retrieved from http://news.bbc.co.uk/1/hi/uk_politics/8361943.stm

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, *6*(2), 1–6. https://doi.org/10.1177/2053951719855091

BEIS. (2018). *Modernising consumer markets: Green paper*. Department for Business, Energy and Industrial Strategy. Retrieved from https://www.gov.uk/government/consultations/consumer-green-paper-modernising-consumer-markets

Bell, Daniel. (1973). *The Coming of Post-Industrial Society*. New York: Basic Books.

Bell, Duncan. (2014). What Is Liberalism? *Political Theory*, *42*(6), 682–715. https://doi.org/gjspjw

Bellamy, C, & Taylor, JA. (1994). Reinventing government in the information age. *Public Money & Management*, *14*(3), 59–62. https://doi.org/10.1080/09540969409387830

Bennett, A. (2020). *Digital Identity: The Missing Piece of the Government's Exit Strategy*. Tony Blair Institute for Global Change.

Bennett, A, & Beverton-Palmer, M. (2020). *Digital Identity: Where Are We, and Where Are We Going?* London, UK: Tony Blair Institute for Global Change. Retrieved from https://institute.global/policy/digital-identity-where-are-we-and-where-are-we-going

Bennett, A, & Beverton-Palmer, M. (2021). *Social Media Futures: How to Reconcile Anonymity, Abuse and Identity Online*. Tony Blair Institute for Global Change. Retrieved from https://institute.global/policy/social-media-futures-anonymity-abuse-and-identity-online

Bennett, CJ, & Lyon, D (Eds.). (2008). *Playing the identity card: Surveillance, security and identification in global perspective*. New York: Routledge.

Bentham, J. (2010). *The Panopticon Writings*. (M. Božovič, Ed.). Verso Books.

Bentham, J, & Quinn, M. (2001). *Writings on the poor laws*. Oxford: Clarendon.

Berlin, I. (2002). *Liberty*. Oxford University Press.

Bernholz, L, Landemore, H, & Reich, R. (2021). Introduction. In *Digital Technology and Democratic Theory* (pp. 1–22). University of Chicago Press. https://doi.org/10.7208/chicago/9780226748603.001.0001

Bertino, E, & Takahashi, K. (2011). *Identity management: Concepts, technologies, and systems*. Boston: Artech House.

Bevan, G. (2023). *How Did Britain Come to This? A century of systemic failures of governance*. LSE Press. https://doi.org/10.31389/lsepress.hdb

Beveridge, W. (1942). *Social Insurance and Allied Services (Beveridge Report)*. London: HM Stationery Office. Retrieved from http://archive.org/details/in.ernet.dli.2015.275849

Big Brother Watch. (2023). *CBDC - a privacy-eroding pound? Lessons from international central bank digital currency pilots for the UK*. Big Brother Watch. Retrieved from https://bigbrotherwatch.org.uk/wp-content/uploads/2023/11/CBDC-a-privacy-eroding-pound-FINAL-1.pdf

Birch, D. (2008). Psychic ID: A blueprint for a modern national identity scheme. *Identity in the Information Society*, *1*(1), 189–201. https://doi.org/10.1007/s12394-009-0014-6

Birch, D. (2014). *Identity Is the New Money*. London: London Publishing Partnership.

Black, E. (2001). *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*. London: Little, Brown and Company.

Bohm, N, & Mason, S. (2010). Identity and its verification. *Computer Law & Security Review*, *26*(1), 43–51. https://doi.org/10.1016/j.clsr.2009.11.003

Bonneau, J, & Preibusch, S. (2010). The password thicket: Technical and market failures in human authentication on the web. In *WEIS 2010: The Ninth Workshop on the Economics of Information Security*.

Borgogno, O, & Colangelo, G. (2020, January 3). Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking [SSRN Scholarly Paper]. https://doi.org/10.2139/ssrn.3513514

Borkin, S. (2019). *Platform co-operatives – solving the capital conundrum*. Nesta.

Bovens, M, & Zouridis, S. (2002). From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control. *Public Administration Review*, *62*(2), 174–184. https://doi.org/10.1111/0033-3352.00168

boyd, danah. (2007). Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. In D. Buckingham (Ed.), *Youth, Identity, and Digital Media* (pp. 119–142). MIT Press. https://doi.org/10.31219/osf.io/22hq2

Braman, S. (2006). *Change of state: Information, policy, and power*. Cambridge, Mass: MIT Press.

Brandão, LTAN, Christin, N, Danezis, G, & Anonymous. (2015). Toward Mending Two Nation-Scale Brokered Identification Systems. *Proceedings on Privacy Enhancing Technologies*, *2015*(2), 135–155. https://doi.org/10.1515/popets-2015-0022

Brandeis, L, & Warren, S. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Brandstedt, E, & Brännmark, J. (2020). Rawlsian Constructivism: A Practical Guide to Reflective Equilibrium. *The Journal of Ethics*, *24*(3), 355–373. https://doi.org/ggvr8n

Breckenridge, K. (2008). The Elusive Panopticon: The HANIS Project and the Politics of Standards in South Africa. In C. J. Bennett & D. Lyon (Eds.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (pp. 39–56). London: Routledge.

Breckenridge, K. (2014). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present*. New York: Cambridge University Press.

Breckenridge, K, & Szreter, S (Eds.). (2012). *Registration and Recognition: Documenting the Person in World History*. Oxford: British Academy. https://doi.org/10.5871/bacad/9780197265314.001.0001

Bridges, LE. (2024). Competing digital capacities: Between state-led digital governance and local data center tradeoffs. *Information, Communication & Society*, (0), 1–18. https://doi.org/10.1080/1369118X.2024.2331765

Brock, DW, & Daniels, N. (1994). Ethical Foundations of the Clinton Administration's Proposed Health Care System. *JAMA*, *271*(15), 1189–1196. https://doi.org/bzpng6

Brooks, R, & Wallis, N. (2020, May). Justice Lost in the Post – Special Report. *Private Eye*. Retrieved from https://www.private-eye.co.uk/special-reports/justice-lost-in-the-post

Brostoff, S, Jennett, C, Malheiros, M, & Sasse, MA. (2013). Federated identity to access e-government services: Are citizens ready for this? In *Proceedings of the 2013 ACM workshop on Digital identity management* (pp. 97–108). New York, NY, USA: Association for Computing Machinery. https://doi.org/ghkh33

Brown, Alan W, McDermid, JA, Sommerville, I, & Witty, R. (2013). A Perspective on the Government Digital Strategy (GDS): Balancing agility and efficiency in UK Government IT delivery. *UK GaaP*. Retrieved from https://ukgaap.weebly.com/gds-critique.html

Brown, Alan W, Thompson, M, & Fishenden, J. (2014). *Digitizing government: Understanding and implementing new digital business models*. Houndmills, Basingstoke, Hampshire ; New York, NY: Palgrave Macmillan.

Brown, G. (2007, October 25). In full: Brown speech on liberty. *BBC*. Retrieved from http://news.bbc.co.uk/1/hi/uk_politics/7062237.stm

Brown, W. (2015). *Undoing the Demos: Neoliberalism's stealth revolution* (First Edition). New York: Zone Books.

Bryman, A. (2012). *Social research methods* (4th ed). Oxford ; New York: Oxford University Press.

Bullingham, L, & Vasconcelos, AC. (2013). "The presentation of self in the online world": Goffman and the study of online identities. *Journal of Information Science*, *39*(1), 101–112. https://doi.org/10.1177/0165551512470051

Burghart, A. Hansard, Written Statement – Closure of GOV.UK Verify, vol 723 (2023). Retrieved from https://hansard.parliament.uk/Commons/2023-05-02/debates/23050217000008/ClosureOfGovUKVerify

Burns, H. (2021, September 17). Papers please: Nationality checks for the British internet? Retrieved August 25, 2024, from https://www.openrightsgroup.org/blog/papers-please-nationality-checks-for-the-british-internet/

Burr, C, & Cristianini, N. (2019). Can Machines Read our Minds? *Minds and Machines*, *29*(3), 461–494. https://doi.org/10.1007/s11023-019-09497-4

Cabinet Office. (2010). *The Coalition: Our programme for government*. HM Government.

Cabinet Office. (2022). *One Login for Government Accounting Officer assessment*. Retrieved from https://www.gov.uk/government/publications/cabinet-office-accounting-officer-assessments/20-september-2022-one-login-for-government-accounting-officer-assessment

Cabinet Office. (2023). Consultation on draft legislation to support identity verification. Retrieved March 23, 2024, from https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/consultation-on-draft-legislation-to-support-identity-verification

Cameron, K. (2005, May). The Laws of Identity. Microsoft. Retrieved from https://www.identityblog.com/?p=352

Caplan, J. (2001). The State in the Field: Official Knowledge and Truant Practices. *The American Historical Review*, *106*(1), 107–113. https://doi.org/10.2307/2652227

Caplan, J, & Torpey, J (Eds.). (2001). *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton, NJ: Princeton University Press.

Capurro, R, Eldred, M, & Nagel, D. (2013). *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld*. Berlin, Boston: DE GRUYTER. https://doi.org/10.1515/9783110320428

Carens, JH. (2013). *The Ethics of Immigration*. New York: Oxford University Press.

Carran, M. (2018). *Consumer Protection in EU Online Gambling Regulation*. European Gaming and Betting Association. Retrieved from https://www.egba.eu/uploads/2018/12/181206-Consumer-Protection-in-EU-Online-Gambling-EBGA-Report-December-2018.pdf

Carter, I. (1995). The Independent Value of Freedom. *Ethics*, *105*(4), 819–845. https://doi.org/10.1086/293754

Casassas, D, & De Wispelaere, J. (2016). Republicanism and the political economy of democracy. *European Journal of Social Theory*, *19*(2), 283–300. https://doi.org/ghgn4v

Castells, M. (2009a). *End of millennium* (2nd Edition). Malden, MA: Blackwell.

Castells, M. (2009b). *The power of identity* (2nd ed). Malden, Mass: Blackwell Pub.

Castells, M. (2009c). *The rise of the network society* (2nd Ed.). Oxford ; Malden, Mass: Blackwell Publishers.

Central IT Unit. (2000, March). Information Age Government 'authentication framework' (version 1.0). Retrieved from https://ntouk.files.wordpress.com/2019/06/authentication-framework-version-1.0.pdf

Chadwick, DW. (2009). Federated Identity Management. In A. Aldini, G. Barthe, & R. Gorrieri (Eds.), *Foundations of Security Analysis and Design V* (Vol. 5705, pp. 96–120). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03829-7_3

Chandler, J. (2009). Privacy Versus National Security: Clarifying the Trade-Off. In I. Kerr, V. M. Steeves, & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, privacy, and identity in a networked society* (pp. 303–318). Oxford University Press.

Chango, M. (2012). *Becoming Artifacts: Medieval Seals, Passports and the Future of Digital Identity* (Doctoral Thesis). Syracuse University. Retrieved from https://surface.syr.edu/it_etd/74

Chango, M. (2022). Building a Credential Exchange Infrastructure for Digital Identity: A Sociohistorical Perspective and Policy Guidelines. *Frontiers in Blockchain*, *4*, 1–27. https://doi.org/10.3389/fbloc.2021.629790

Cheesman, M. (2022a). *Infrastructure Justice and Humanitarianism: Blockchain's Promises in Practice*. University of Oxford.

Cheesman, M. (2022b). Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. *Geopolitics*, *27*(1), 134–159. https://doi.org/10.1080/14650045.2020.1823836

Cheney-Lippold, J. (2011). A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, *28*(6), 164–181. https://doi.org/10.1177/0263276411424420

Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York: New York University Press.

Chilson, N. (2021). Seeing (Platforms) Like a State: Digital Legibility and Lessons for Platform Governance, *Catholic University Journal of Law and Technology 29*(2), 31–62. https://scholarship.law.edu/jlt/vol29/iss2/4/

Cifas. (2024). *Fraudscape 2024 (6 Month Update)*. Cifas. Retrieved from https://cdn.prod.website-files.com/5f24212f91518a2cd44d736f/66bb503c6dcb4330ed45c674_Fraudscape%206%20month%20update-12.08.pdf

Clarke, J, & Newman, J. (2007). What's in a Name?: New Labour's citizen-consumers and the remaking of public services. *Cultural Studies*, *21*(4-5), 738–757. https://doi.org/10.1080/09502380701279051

Coalition Agreement. (2010, May 13). Conservative-Liberal Democrat Coalition Negotiations: Agreements Reached. The Conservatives. Retrieved from https://web.archive.org/web/20100513201736/http://www.conservatives.com/~/media/Files/Downloadable%20Files/agreement.ashx?dl=true

Cobbe, J. (2018). *Big Data, Surveillance, and the Digital Citizen*. Retrieved from https://www.ssrn.com/abstract=3234984

Coeckelbergh, M. (2018). Technology and the good society: A polemical essay on social ontology, political principles, and responsibility for technology. *Technology in Society*, *52*, 4–9. https://doi.org/10.1016/j.techsoc.2016.12.002

Coeckelbergh, M. (2022). *The political philosophy of AI: An introduction*. Cambridge: Polity.

Cohen, JE. (2012). Configuring the Networked Citizen. In *Imagining New Legalities* (pp. 129–153). Stanford University Press. https://doi.org/10.11126/stanford/9780804777049.003.0005

Coles-Kemp, L, & Heath, C. (2020). *Digital Identity: Ground-up Perspectives*. Royal Holloway University of London. Retrieved from https://pure.royalholloway.ac.uk/ws/portalfiles/portal/39967033/Digital_Identity_Ground_up_Perspectives_DCMSRHUL_2020.pdf

Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID). *Information Security Technical Report*, 10. https://doi.org/10.1016/j.istr.2008.06.002

Conover, PJ. (1995). Citizen Identities and Conceptions of the Self*. *Journal of Political Philosophy*, *3*(2), 133–165. https://doi.org/10.1111/j.1467-9760.1995.tb00032.x

Cook, C. (2014, December 17). A Christmas government website wish. *BBC News: UK Politics*. Retrieved from https://www.bbc.com/news/uk-politics-30524570

Co-Operative Group. (2010, June 17). The Co-operative Group members share record £50 million dividend. Retrieved September 7, 2024, from https://www.co-operative.coop/media/news-releases/the-co-operative-group-members-share-record-50million-dividend

Couldry, N, & Mejias, UA. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, California: Stanford University Press.

Cox, J. (2024, February 5). Inside the Underground Site Where "Neural Networks" Churn Out Fake IDs. Retrieved March 30, 2024, from https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

Crenshaw, K. (1989). Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics. *University of Chicago Legal Forum*, *1989*(1), 57–80.

Crosby, J. (2008). *Challenges and opportunities in identity assurance*. London: HM Treasury.

Crowder, G. (1998). From value pluralism to liberalism. *Critical Review of International Social and Political Philosophy*, *1*(3), 2–17. https://doi.org/10.1080/13698239808403245

Curry, A. (2008, January 18). Piecing Together the Dark Legacy of East Germany's Secret Police. *Wired*. Retrieved from https://www.wired.com/2008/01/ff-stasi/

D'Agostino, F, Gaus, G, & Thrasher, J. (2024). Contemporary Approaches to the Social Contract. In E. N. Zalta & U. Nodelman (Eds.), *The Stanford Encyclopedia of Philosophy* (Spring 2024). Metaphysics Research Lab, Stanford University. Retrieved from https://plato.stanford.edu/archives/spr2024/entries/contractarianism-contemporary/

Daniels, N. (1979). Wide Reflective Equilibrium and Theory Acceptance in Ethics. *The Journal of Philosophy*, *76*(5), 256–282. https://doi.org/cb2h6n

Daniels, N. (1996). *Justice and Justification: Reflective Equilibrium in Theory and Practice*. Cambridge, GBR: Cambridge University Press. Retrieved from http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4637016

Davis, JL. (2020). *How artifacts afford: The power and politics of everyday things*. Cambridge, MA: The MIT Press.

DCMS. (2020, September). Government response to the digital identity and attributes consultation - GOV.UK. Retrieved March 20, 2022, from https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/outcome/government-response-to-the-digital-identity-and-attributes-consultation

DCMS. (2021, February 11). The UK digital identity and attributes trust framework. Retrieved from https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

DCMS. (2022a). *UK Digital Strategy*. Retrieved from https://www.gov.uk/government/publications/uks-digital-strategy

DCMS. (2022b, June 13). UK digital identity and attributes trust framework beta version (0.3). Retrieved August 23, 2024, from https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version

DCMS. (2023, February). Government response to the digital identity and attributes consultation. Retrieved March 8, 2024, from https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/outcome/government-response-to-the-digital-identity-and-attributes-consultation

DCMS, & Office, C. (2019). Digital Identity: Call for Evidence. *Consultation July 2019*. Retrieved from https://www.gov.uk/government/consultations/digital-identity

De Gregorio, G. (2022). *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781009071215

De Hert, PJA. (2008). A right to identity to face the internet of things? Retrieved from https://research.tilburguniversity.edu/en/publications/a-right-to-identity-to-face-the-internet-of-things

de Laat, PB. (2018). Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability? *Philosophy & Technology*, *31*(4), 525–541. https://doi.org/10.1007/s13347-017-0293-z

de-Shalit, A. (2009). Political Philosophy and Empirical Political Science: From Foes to Friends? *European Political Science*, *8*(1), 37–46. https://doi.org/fqk388

de Vries, K. (2010). Identity, profiling algorithms and a world of ambient intelligence. *Ethics and Information Technology*, *12*(1), 71–85. https://doi.org/10.1007/s10676-009-9215-9

De Vries, M, & Van Leeuwen, E. (2009). Reflective Equilibrium and Empirical Data: Third Person Moral Experiences in Empirical Medical Ethics. *Bioethics*, *24*(9), 490–498. https://doi.org/dj64xt

Debos, M. (2021). Biometrics and the disciplining of democracy: Technology, electoral politics, and liberal interventionism in Chad. *Democratization*, *28*(8), 1–17. https://doi.org/gkbfzz

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, *59*, 3–7. Retrieved from http://www.jstor.org/stable/778828

Derrida, J. (1997). *The Politics of Friendship*. London: Verso.

Desrosières, A. (2010). *The Politics of Large Numbers: A History of Statistical Reasoning*. (C. Naish, Trans.). Cambridge, Mass.: Harvard University Press.

Dixon, J, & Hyde, M. (2009). Citizenship, the Public Interest and Governance. In A. Kakabadse, N. Kakabadse, & K. N. Kalu (Eds.), *Citizenship: A Reality Far From Ideal* (pp. 63–80). London: Palgrave Macmillan UK. https://doi.org/10.1057/9780230244887_5

Dmytrenko, O, & Nardali, A. (2005).Net Passport Under the Scrutiny of U.S. And EU Privacy Law: Implications for the Future of Online Authentication. *IS: A Journal of Law and Policy for the Information Society*, *1*(2), 619–645.

Doorn, N. (2009). Applying Rawlsian Approaches to Resolve Ethical Issues: Inventory and Setting of a Research Agenda. *Journal of Business Ethics*, *91*(1), 127–143. https://doi.org/d6bg44

Doorn, N, & Taebi, B. (2018). Rawls's Wide Reflective Equilibrium as a Method for Engaged Interdisciplinary Collaboration: Potentials and Limitations for the Context of Technological Risks. *Science, Technology, & Human Values*, *43*(3), 487–517. https://doi.org/gcz7v8

DPDI. Data Protection and Digital Information Bill (2024).

Driver's license. (2024, August 31). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Driver%27s_license&oldid=1243293069#References

Dryzek, JS, & Dunleavy, P. (2009). *Theories of the democratic state*. Basingstoke, Hampshire: Palgrave Macmillan.

DSIT. (2024a). *Good Practice Guide 45: Validating and Verifying the identity of an individual*. Retrieved from https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity

DSIT. (2024b). *Public dialogue on trust in digital identity services: A findings report*. Retrieved from https://www.gov.uk/government/publications/public-dialogue-on-trust-in-digital-identity-services/public-dialogue-on-trust-in-digital-identity-services-a-findings-report

DSIT. (2024c, July 8). DSIT bolstered to better serve the British public through science and technology. Retrieved August 25, 2024, from https://www.gov.uk/government/news/dsit-bolstered-to-better-serve-the-british-public-through-science-and-technology

DSIT. (2024d, August 23). List of certified digital identity and attribute services. Retrieved August 25, 2024, from https://www.gov.uk/government/publications/list-of-certified-digital-identity-and-attribute-services

Dunleavy, P, Margetts, H, Tinkler, J, & Bastow, S. (2006). *Digital Era Governance: IT Corporations, the State, and E-Government*. OUP Oxford. Retrieved from https://books.google.com?id=HLcUDAAAQBAJ

Dusek, V. (2006). *Philosophy of technology: An introduction*. Malden, MA ; Oxford: Blackwell Pub.

DVLA. (2021). *Driving Change: DVLA Strategic Plan 2021 - 24*. Driver and Vehicle Licencing Agency.

DWP. (2020, October 15). Confirm Your Identity: A new way to verify online. Retrieved October 27, 2020, from https://dwpdigital.blog.gov.uk/2020/10/15/confirm-your-identity-a-new-way-to-verify-online/

Eaton, J. (1999). "Open, Sesame?" – the problems of digital identity and secure access to information in the Internet era: Issues for the information industry. *Business Information Review*, *16*(4), 184–191. https://doi.org/10.1177/0266382994237342

Eaves, D, Pope, R, & McGuire, B. (2019). Government as a Platform: How Policy Makers Should Think about the Foundations of Digital Public Infrastructure. *Kennedy School Review*, *19*(1), 126–131.

Edwardes, CA, Hosein, I, & Whitley, EA. (2007). Balance, scrutiny and identity cards in the UK. *Criminal Justice Matters*, *68*(1), 29–30. https://doi.org/10.1080/09627250708553282

Edwards, R, & Holland, J. (2013). How have qualitative interviews developed? In *What is qualitative interviewing?* (pp. 11–28). Bloomsbury Academic.

Elgin, CZ. (1999). *Considered Judgment*. Princeton University Press. Retrieved from https://press.princeton.edu/books/paperback/9780691005232/considered-judgment

Elliot, R. (2006). An Early Experiment in National Identity Cards: The Battle Over Registration in the First World War. *Twentieth Century British History*, *17*(2), 145–176. https://doi.org/10.1093/tcbh/hwl006

Etherington, D. (2020). Embedding neoliberal austerity: From New Labour to the Conservative government. In D. Etherington (Ed.), *Austerity, Welfare and Work: Exploring Politics, Geographies and Inequalities* (pp. 47–70). Policy Press. https://doi.org/10.1332/policypress/9781447350088.003.0003

Evenstad, L. (2018, August 15). Scotland's Improvement Service signs up to pilot digital identity platform. Retrieved August 22, 2024, from https://www.computerweekly.com/news/252446915/Scotlands-Improvement-Service-signs-up-to-pilot-digital-identity-platform

Evenstad, L. (2020a, August 10). Government launches digital identity checking pilot. Retrieved August 23, 2024, from https://www.computerweekly.com/news/252487406/Government-launches-digital-identity-checking-pilot

Evenstad, L. (2020b, August 10). Gov.uk Verify continues to pose "notable risk" to Cabinet Office. Retrieved November 19, 2020, from https://www.computerweekly.com/news/252487391/Govuk-Verify-continues-to-pose-notable-risk-to-Cabinet-Office

Experian. (2019, July 23). What to Know About the Effects of Identity Theft. Retrieved August 18, 2024, from https://www.experian.com/blogs/ask-experian/how-long-can-the-effects-of-identity-theft-last/

Falcão-Reis, F, & Correia, ME. (2010). Patient Empowerment by the Means of Citizen-managed Electronic Health Records: Web 2.0 Health Digital Identity scenarios. In *Medical and Care Compunetics 6* (pp. 214–228). IOS Press. https://doi.org/10.3233/978-1-60750-565-5-214

Feher, K. (2019). Digital identity and the online self: Footprint strategies – An exploratory and comparative research study. *Journal of Information Science*, 1–14. https://doi.org/10.1177/0165551519879702

Ferlie, E. (2017). The New Public Management and Public Management Studies. In *Oxford Research Encyclopedia of Business and Management*. https://doi.org/10.1093/acrefore/9780190224851.013.129

Fishenden, J. (2005). eID: Identity Management in an Online World. In *5th European Conference on e-Government* (pp. 1–12).

Fishenden, J. (2020). Federated Identity for Access to UK Public Services: 1997-2020. Retrieved May 3, 2021, from https://ntouk.wordpress.com/wp-content/uploads/2020/06/federated-identity-for-access-to-uk-public-services-1997-2020-jerry-fishenden-1.pdf

Fishenden, J, & Mather, A. (2021, January 25). Government Gateway at 20 – looking back at the UK's most successful digital identity system. Retrieved January 25, 2021, from https://www.computerweekly.com/opinion/Government-Gateway-at-20-looking-back-at-the-UKs-most-successful-digital-identity-system

Fishenden, J, & Thompson, M. (2013). Digital Government, Open Architecture, and Innovation: Why Public Sector IT Will Never Be the Same Again. *Journal of Public Administration Research and Theory*, *23*(4), 977–1004. https://doi.org/gfz9v7

Flood, G. (2023, October 4). Home Office award contract for digital registrations service. *UKAuthority*. Retrieved from https://www.ukauthority.com/articles/home-office-award-contract-for-digital-registrations-service/

Floridi, L, Cowls, J, Beltrametti, M, Chatila, R, Chazerand, P, Dignum, V, *et al.*Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, *28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Floyd, J. (2017). Rawls' methodological blueprint. *European Journal of Political Theory*, *16*(3), 367–381. https://doi.org/ghnft9

Flyverbom, M. (2019). *The digital prism: Transparency and visibility in the age of total information*. New York: Cambridge University Press.

Foley, B. (2017). *Delivering on Universal Credit*. Citizens Advice. Retrieved from https://www.citizensadvice.org.uk/Global/CitizensAdvice/welfare%20publications/Delivering%20on%20Universal%20Credit%20-%20report.pdf

Forrester, K. (2019). *In the Shadow of Justice: Postwar Liberalism and the Remaking of Political Philosophy* (1st edition). Princeton, NJ: Princeton University Press.

Foucault, M. (1980). *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*. Knopf Doubleday Publishing Group. Retrieved from https://books.google.com?id=Aqf309sk_EsC

Foucault, M. (1991). *Discipline and Punish: The Birth of the Prison*. (A. Sheridan, Trans.). London: Penguin.

Fourcade, M. (2021). Ordinal citizenship. *The British Journal of Sociology*, *72*(2), 154–173. https://doi.org/10.1111/1468-4446.12839

Fourcade, M, & Gordon, J. (2020). Learning Like a State: Statecraft in the Digital Age. *Journal of Law and Political Economy*, *1*(1), 78–108. Retrieved from https://escholarship.org/uc/item/3k16c24g

Francis, S. (2023, June 23). ID rules stopped 14,000 people voting, watchdog finds. *BBC News: UK Politics*. Retrieved from https://www.bbc.com/news/uk-politics-65988959

Freeden, M (Ed.). (1986). *The New Liberalism: An Ideology of Social Reform*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198229612.002.0003

Freeguard, G, & Shepheard, M. (2020). *Digital government during the coronavirus crisis*. Institute for Government. Retrieved from https://www.instituteforgovernment.org.uk/sites/default/files/publications/digital-government-coronavirus.pdf

Fuchs, C. (2013). Political Economy and Surveillance Theory. *Critical Sociology*, *39*(5), 671–687. https://doi.org/10.1177/0896920511435710

Galston, WA. (1999). Value Pluralism and Liberal Political Theory. *The American Political Science Review*, *93*(4), 769–778. https://doi.org/10.2307/2586111

Gandy, OH. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colo: Westview.

Gangadharan, SP. (2021). Digital Exclusion: A Politics of Refusal. In L. Bernholz (Ed.), *Digital Technology and Democratic Theory* (pp. 113–140). Chicago University Press.

GDS. (2011, November 4). Establishing trust in digital services. Retrieved August 14, 2024, from https://gds.blog.gov.uk/2011/11/04/establishing-trust/

GDS. (2012, March 1). Identity: One small step for all of Government. Retrieved August 14, 2024, from https://gds.blog.gov.uk/2012/03/01/identity-a-small-step/

GDS. (2014a, January 23). What is identity assurance? Retrieved August 5, 2024, from https://gds.blog.gov.uk/2014/01/23/what-is-identity-assurance/

GDS. (2014b, April 23). User needs and revolutions. Retrieved August 13, 2024, from https://gds.blog.gov.uk/2014/04/23/user-needs-and-revolutions/

GDS. (2014c, November 5). How the GOV.UK Verify technical architecture protects users' privacy, and why it's appropriate. Retrieved August 13, 2024, from https://identityassurance.blog.gov.uk/2014/11/05/tech-arch-privacy/

GDS. (2017, February 1). Growing Verify: Services that need less proof of identity. Retrieved August 15, 2024, from https://identityassurance.blog.gov.uk/2017/02/01/growing-verify-services-that-need-less-proof-of-identity/

GDS. (2021, March 15). GOV.UK Verify Dashboard. Retrieved March 16, 2021, from https://webarchive.nationalarchives.gov.uk/ukgwa/20210315091743mp_/https://www.gov.uk/performance/govuk-verify/users-accessing-services

GDS. (2023, November). One Login Inclusion and Privacy Advisory Group. Retrieved September 7, 2024, from https://www.gov.uk/government/groups/one-login-inclusion-and-privacy-advisory-group

GDS. (2024). Checking users' identities - GOV.UK One Login. Retrieved April 7, 2024, from https://www.sign-in.service.gov.uk/about/checking-users-identities

Gelb, A, & Diofasi Metz, A. (2018). *Identification revolution: Can digital ID be harnessed for development?* Washington, D.C: Center for Global Development.

Gellman, B. (2023, May 17). NSA tracking cellphone locations worldwide, Snowden documents show. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

Gibbs, E, McCartney, G, & Phillips, J. (2024). The Fundamentals of Public Ownership: Learning from UK Historical Experience and Recent Scottish Policy. *The Political Quarterly*, *95*(1), 157–166. https://doi.org/10.1111/1467-923X.13348

Gillespie, M, Osseiran, S, & Cheesman, M. (2018). Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances. *Social Media + Society*, *4*(1), 1–12. https://doi.org/gc8znb

Glick, B. (2014, September 16). GDS unveils 'Gov.UK Verify' public services identity assurance scheme. Retrieved July 6, 2024, from https://www.computerweekly.com/news/2240230648/GDS-unveils-GovUK-Verify-public-services-identity-assurance-scheme

Glick, B. (2018, October 9). Government to end investment in Gov.uk Verify digital identity system. Retrieved September 9, 2020, from https://www.computerweekly.com/news/252450313/Government-to-end-investment-in-Govuk-Verify-digital-identity-system

Glick, B. (2019a, March 6). NAO hammers another nail into Gov.uk Verify - Computer Weekly Editor's Blog. Retrieved October 27, 2020, from https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/NAO-hammers-another-nail-into-Govuk-Verify

Glick, B. (2019b, August 5). Why Gov.uk Verify faces a critical few months - again. Retrieved March 3, 2024, from https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/Why-Govuk-Verify-faces-a-critical-few-months-again

Glick, B. (2019c, August 23). Three more identity providers to withdraw from troubled Gov.uk Verify programme. Retrieved November 5, 2019, from https://www.computerweekly.com/news/252469110/Three-more-identity-providers-to-withdraw-from-troubled-Govuk-Verify-programme

Glick, B. (2020a, May 1). Treasury gives Gov.uk Verify 18-month reprieve due to coronavirus. Retrieved May 1, 2020, from https://www.computerweekly.com/news/252482534/Treasury-gives-Govuk-Verify-18-month-reprieve-due-to-coronavirus

Glick, B. (2020b, May 7). HM Treasury tells GDS: No further online services can use Gov.uk Verify. Retrieved May 7, 2020, from https://www.computerweekly.com/news/252482828/HM-Treasury-tells-GDS-no-further-online-services-can-use-Govuk-Verify

Glick, B. (2020c, July 30). Tech sector calls on government to 'urgently' resolve delays in digital identity policy. Retrieved July 30, 2020, from https://www.computerweekly.com/news/252486858/Tech-sector-calls-on-government-to-urgently-resolve-delays-in-digital-identity-policy

Glick, B. (2020d, November 24). What next for digital identity in the UK? Industry welcomes latest DCMS plan. Retrieved August 24, 2024, from https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/What-next-for-digital-identity-in-the-UK-Industry-welcomes-latest-DCMS-plan

Glick, B. (2021a, February 15). Government to impose new digital identity system across all Gov.uk services. Retrieved August 24, 2024, from https://www.computerweekly.com/news/252496337/Government-to-impose-new-digital-identity-system-across-all-Govuk-services

Glick, B. (2021b, June 8). CIO interview: Tom Read, chief executive, Government Digital Service. Retrieved June 8, 2021, from

https://www.computerweekly.com/news/252501808/CIO-interview-Tom-Read-chief-executive-Government-Digital-Service

Glick, B. (2021c, October 25). At last, the UK has a mass-market digital identity system - now let's use it. Retrieved August 24, 2024, from https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/At-last-the-UK-has-a-mass-market-digital-identity-system-now-lets-use-it

Glick, B. (2021d, October 29). GDS secures up to £400m funding for One Login digital identity project. Retrieved August 24, 2024, from https://www.computerweekly.com/news/252508823/GDS-secures-400m-funding-for-One-Login-digital-identity-project

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Anchor Books.

Goldsmith, JL, & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. New York: Oxford University Press.

Goodin, RE. (1992). *Political theory and public policy*. Chicago University Press.

Goodman, N. (1955). *Fact, Fiction, and Forecast*. Cambridge, Mass: Harvard University Press.

Gorski, PS. (2003). *The disciplinary revolution: Calvinism and the rise of the state in early modern Europe*. Chicago: University of Chicago Press.

Government as a Platform in Practice: Commonalities and Differences Across Three European Countries. (2023). In P. Kuhn, G. Maragno, D. Balta, L. Gastaldi, & F. Matthes, *Lecture Notes in Computer Science* (pp. 34–47). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-41138-0_3

Grayson, TRD. (2003). Philosophy of Identity. *Self-Published*, 6.

Groebner, V. (2007). *Who Are You?* Princeton University Press. Retrieved from https://press.princeton.edu/books/hardcover/9781890951726/who-are-you

Grossman, W. (1997). *Net.wars*. New York: New York University Press.

Habermas, J. (2005). *Theory of Communicative Action, Volume Two. Lifeworld and system: A critique of functionalist reason*. (T. MacCarthy, Trans.) (1. digital-print ed). Boston: Beacon.

Hadjimatheou, K. (2023). Surveillance, Democracy, and Protest in a Time of Climate Crisis. In K. Macnish & A. Henschke (Eds.), *The Ethics of Surveillance in Times of Emergency* (pp. 132–149). Oxford University Press. https://doi.org/10.1093/oso/9780192864918.003.0009

Haggerty, KD, & Ericson, RV. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Hall, JA. (1985). Capstones and Organisms: Political Forms and the Triumph of Capitalism. *Sociology*, *19*(2), 173–192. https://doi.org/10.1177/0038038585019002003

Halperin, R, & Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the Information Society*, *1*(1), 71–87. https://doi.org/10.1007/s12394-008-0004-0

Hanna, P, & Mwale, S. (2017). "I'm Not 'with' You, Yet I Am …": Virtual Face-to-Face Interviews. In V. Braun, V. Clarke, & D. Gray (Eds.), *Collecting Qualitative Data* (1st ed., pp. 256–274). Cambridge University Press. https://doi.org/10.1017/9781107295094.013

Hansard, HC Deb vol 73 col 108 (July 5, 1915).

Haraway, D. (1988). Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. *Feminist Studies*, *14*(3), 575–599. https://doi.org/10.2307/3178066

Hayek, F. (1948). *Individualism and Economic ORder*. University of Chicago Press.

Hayward, F. (2024, July 6). Keir Starmer appoints a continuity cabinet. *New Statesman*. Retrieved from https://www.newstatesman.com/politics/labour/2024/07/keir-starmer-has-appointed-a-continuity-cabinet

Hendry, S. (2018, January 25). Should England nationalise water services? Retrieved August 31, 2024, from https://blogs.lse.ac.uk/politicsandpolicy/should-england-nationalise-water-services/

Hersey, F. (2023, March 21). Multimillion pound contracts keep coming for UK Government Digital Service's One Login. *Biometric Update*. Retrieved from https://www.biometricupdate.com/202303/multimillion-pound-contracts-keep-coming-for-uk-government-digital-services-one-login

Hicks, M. (2019). Hacking the Cis-tem. *IEEE Annals of the History of Computing*, *41*(1), 20–33. https://doi.org/10.1109/MAHC.2019.2897667

Higgs, E. (2001). The Rise of the Information State: The Development of Central State Surveillance of the Citizen in England, 1500–2000. *Journal of Historical Sociology*, *14*(2), 175–197. https://doi.org/10.1111/1467-6443.00141

Higgs, E. (2004). *The Information State in England: The Central Collection of Information on Citizens Since 1500*. New York, N.Y: Palgrave Macmillan.

Higgs, E. (2009). Change and continuity in the techniques and technologies of identification over the second Christian millennium. *Identity in the Information Society*, *2*(3), 345–354. https://doi.org/10.1007/s12394-009-0035-1

Higgs, E. (2011). *Identifying the English: A History of Personal Identification, 1500 to the Present*. London: Continuum.

Higgs, E. (2013). Consuming Identity and Consuming the State in Britain since c.1750. In I. About, J. Brown, & G. Lonergan (Eds.), *Identification and Registration Practices in Transnational Perspective: People, Papers and Practices* (pp. 164–182). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137367310_11

Hilvert, C, & Swindell, D. (2013). Collaborative Service Delivery: What Every Local Government Manager Should Know. *State and Local Government Review*, *45*(4), 240–254. https://doi.org/10.1177/0160323X13513908

Hind, D. (2019). *The British Digital Cooperative: A New Model Public Sector Institution*. Common Wealth. Retrieved from https://thenextsystem.org/bdc

Hindess, B. (1996). *Discourses of Power: From Hobbes to Foucault*. Oxford: Blackwell.

Hintz, A, & Brown, I. (2017). Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden, 1–20.

HM Government. Licensing Act 2003 (2003). Statute Law Database. Retrieved from https://www.legislation.gov.uk/ukpga/2003/17/contents

HM Treasury. (2006, July 11). Chancellor appoints Sir James Crosby to lead Public Private Forum on Identity. Retrieved August 16, 2024, from https://web.archive.org/web/20090221142837/http://www.hm-treasury.gov.uk/press_51_06.htm

HM Treasury. (2020). *Budget 2020: Delivering on Our Promises to the British People*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/871799/Budget_2020_Web_Accessible_Complete.pdf

HM Treasury. (2023, February 7). The digital pound: A new form of money for households and businesses? Retrieved August 25, 2024, from https://www.gov.uk/government/consultations/the-digital-pound-a-new-form-of-money-for-households-and-businesses

HMPO. (2023, June). Guide to Birth Certificates. HM Passport Office. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1167390/OV_01.2_OV_Birth_certificates_leaflet_Web.pdf

HMPO. (2024). Confirm someone's identity online for a passport application. Retrieved September 7, 2024, from https://www.gov.uk/confirm-identity-online-for-passport-application

Hobbes, T. (1651). *Leviathan: Or the matter, forme and power of a commonwealth ecclasiasticall and civil*. McMaster University Archive.

Hoffmann, AL. (2017). Beyond distributions and primary goods: Assessing applications of rawls in information science and technology literature since 1990. *Journal of the Association for Information Science and Technology*, *68*(7), 1601–1618. https://doi.org/gbkrxh

Hogan, B. (2010). The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society*, *30*(6), 377–386. https://doi.org/10.1177/0270467610385893

Home Office. (2002). *Entitlement Cards and Identity Fraud: A Consultation Paper*. Retrieved from https://image.guardian.co.uk/sys-files/Politics/documents/2002/07/03/idcard.pdf

Home Office. (2006). *Strategic Action Plan for the National Identity Card Scheme: Safeguarding your Identity*. London: Home Office. Retrieved from https://www.dematerialisedid.com/pdfs/strategic_action_plan.pdf

Home Office. (2010, May 27). Identity cards are to be scrapped. Retrieved June 25, 2024, from https://www.gov.uk/government/news/identity-cards-are-to-be-scrapped

Home Office. (2011, February 10). ID Card Database Destroyed. Retrieved November 17, 2020, from https://www.gov.uk/government/news/id-card-database-destroyed

Home Office. (2024, April 17). eVisa rollout begins with immigration documents replaced by 2025. Retrieved September 1, 2024, from https://www.gov.uk/government/news/evisa-rollout-begins-with-immigration-documents-replaced-by-2025

Hood, C. (1991). A Public Management for All Seasons? *Public Administration*, *69*(1), 3–19. https://doi.org/10.1111/j.1467-9299.1991.tb00779.x

Hood, C, & Dixon, R. (2015). *A Government that Worked Better and Cost Less?: Evaluating Three Decades of Reform and Change in UK Central Government*. OUP Oxford. Retrieved from https://books.google.com?id=swjHCQAAQBAJ

Hood, C, & Heald, D (Eds.). (2006). *Transparency: The Key to Better Governance?* Oxford, New York: Oxford University Press.

Hosein, G, & Whitley, E. (2018). Identity and Development: Questioning Aadhaar's Digital Credentials. In R. Khera (Ed.), *Dissent on Aadhaar: Big data meets big brother* (pp. 219–238). Orient Blackswan. Retrieved from http://personal.lse.ac.uk/whitley/allpubs/obs2018.pdf

Hoven, J van den, & Rooksby, E. (2008). Distributive Justice and the Value of Information. In J. van den Hoven & J. Weckert (Eds.), *Information technology and moral philosophy* (pp. 376–396). Cambridge ; New York: Cambridge University Press.

Hoven, J van den, & Weckert, J (Eds.). (2008). *Information technology and moral philosophy*. Cambridge ; New York: Cambridge University Press.

Hoye, JM, & Monaghan, J. (2018). Surveillance, freedom and the republic. *European Journal of Political Theory*, *17*(3), 343–363. https://doi.org/10.1177/1474885115608783

Hübner, D. (2017). Three Remarks on "Reflective Equilibrium": On the Use and Misuse of Rawls' Balancing Concept in Contemporary Ethics. *Philosophical Inquiry*, *41*(1), 11–40. https://doi.org/10.5840/philinquiry20174112

Husz, O. (2018). Bank Identity: Banks, ID Cards, and the Emergence of a Financial Identification Society in Sweden. *Enterprise & Society*, *19*(2), 391–429. https://doi.org/10.1017/eso.2017.43

Infrastructure and Projects Authority. (2023). *Infrastructure and Projects Authority Annual Report 2022-23*. Retrieved from https://www.gov.uk/government/publications/infrastructure-and-projects-authority-annual-report-2022-23

ISI. (2020). *Locked in and Locked Out: The Impact of Digital Identity Systems on Rohingya Populations*. The Institute on Statelessness and Inclusion. Retrieved from https://files.institutesi.org/Locked_In_Locked_Out_The_Rohingya_Briefing_Paper.pdf

Iversen, T. (2021). Democracy and Capitalism. In D. Béland, S. Leibfried, K. J. Morgan, H. Obinger, & C. Pierson (Eds.), *The Oxford Handbook of the Welfare State* (pp. 259–277). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198828389.013.15

Jones, N. (2022, August 24). An update on One Login for Government. Retrieved March 31, 2024, from https://gds.blog.gov.uk/2022/08/24/an-update-on-one-login-for-government/

Joseph, AM. (2001). Anthropometry, the Police Expert, and the Deptford Murders: The Contested Introduction of Fingerprinting for the Identification of Criminals in Late Victorian and Edwardian Britain. In J. Caplan & J. Torpey (Eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton, NJ: Princeton University Press.

Joshi, F. (2020, September 16). UK government plan for digital identity lacks substance and strategy. Retrieved September 16, 2020, from https://www.computerweekly.com/opinion/UK-government-plans-for-digital-identity-lack-substance-and-strategy

Kakabadse, N, Kakabadse, A, & Kalu, KN. (2009). Reconceptualising Citizenship and Identity: Contextual and Attitudinal Responses Towards State and Civic Obligation in the United Kingdom. In A. Kakabadse, N. Kakabadse, & K. N. Kalu (Eds.), *Citizenship: A Reality Far From Ideal* (pp. 101–144). London: Palgrave Macmillan UK. https://doi.org/10.1057/9780230244887_7

Kattel, R, & Takala, V. (2023). The Case of the UK's Government Digital Service: The Professionalisation of a Paradigmatic Public Digital Agency. *Digital Government: Research and Practice*, *4*(4), 1–15. https://doi.org/10.1145/3630024

Kent, ST, Millett, LI, & (U.S.), NRC (Eds.). (2003). *Who goes there? Authentication through the lens of privacy*. Washington, D.C: National Academies Press.

Kerr, I, Steeves, VM, & Lucock, C (Eds.). (2009). *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society*. Oxford, UK: Oxford University Press.

Khera, R (Ed.). (2019). *Dissent on Aadhaar: Big data meets big brother*. Hyderabad, Telangana: Orient BlackSwan.

Kiser, M. (2024). Ethics for Digital Identity and Identity-Driven Algorithms. *IDPro Body of Knowledge*, *1*(14), 1–11. https://doi.org/10.55621/idpro.105

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*. Los Angeles, California: SAGE Publications.

Knight, C. (2017). Reflective Equilibrium. In A. Blau, *Methods in Analytical Political Theory* (pp. 46–64). Cambridge University Press.

Kormann, DP, & Rubin, AD. (2000). Risks of the Passport single signon protocol. *Computer Networks*, *33*(1), 51–58. https://doi.org/10.1016/S1389-1286(00)00048-7

Krajewska, M. (2017). *Documenting Americans: A Political History of National ID Card Proposals in the United States* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781108186773

Kreiss, D, & McGregor, SC. (2018). Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle. *Political Communication*, *35*(2), 155–177. https://doi.org/10.1080/10584609.2017.1364814

Kuhnle, S, & Sander, A. (2021). The Emergence of the Western Welfare State. In D. Béland, S. Leibfried, K. J. Morgan, H. Obinger, & C. Pierson (Eds.), *The Oxford Handbook of the Welfare State* (p. 0). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198828389.013.5

Kukathas, C. (1996). Liberalism, Communitarianism, and Political Community. *Social Philosophy and Policy*, *13*(1), 80–104. https://doi.org/10.1017/S0265052500001539

Kymlicka, W. (1996). *Multicultural Citizenship: A Liberal Theory of Minority Rights*. Oxford University Press. https://doi.org/10.1093/0198290918.001.0001

Lasswell, HD. (1950). *Politics: Who gets what, when, how*. New York: P. Smith. Retrieved from https://bac-lac.on.worldcat.org/oclc/1019293257

Latour, B. (1993). *We have never been modern*. Cambridge, Mass: Harvard University Press.

Lau, DT, Sosa, P, Dasgupta, N, & He, H. (2021). Impact of the COVID-19 Pandemic on Public Health Surveillance and Survey Data Collections in the United States. *American Journal of Public Health*, *111*(12), 2118–2121. https://doi.org/10.2105/AJPH.2021.306551

Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. Cambridge, Massachusetts: The MIT Press.

Leopold, D, & Stears, M (Eds.). (2008). *Political theory: Methods and approaches*. Oxford ; New York: Oxford University Press.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.

Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.

Lewis, DK. (1983). *Philosophical Papers* (Vol. 1). Oxford University Press.

Lips, AMB. (2006). E-government under construction: Challenging traditional conceptions of citizenship. In P. G. Nixon & V. N. Koutrakou, *E-government in Europe: Re-booting the State* (pp. 61–75). Routledge. https://doi.org/10.4324/9780203962381-14

Lips, AMB. (2010). Rethinking citizen - government relationships in the age of digital identity: Insights from research. *Information Polity: The International Journal of Government & Democracy in the Information Age*, *15*(4), 273–289. https://doi.org/10.3233/IP-2010-0216

Lips, AMB. (2013). Reconstructing, attributing and fixating citizen identities in digital-era government. *Media, Culture & Society*, *35*(1), 61–70. https://doi.org/ghccmq

Lips, AMB, Taylor, JA, & Organ, J. (2009a). Identity Management, Administrative Sorting and Citizenship in New Modes of Government. *Information, Communication & Society*, *12*(5), 715–734. https://doi.org/10.1080/13691180802549508

Lips, AMB, Taylor, JA, & Organ, J. (2009b). Managing Citizen Identity Information in E-Government Service Relationships in the UK. *Public Management Review*, *11*(6), 833–856. https://doi.org/10.1080/14719030903318988

List, C, & Valentini, L. (2016). The Methodology of Political Theory. In H. Cappelen, T. S. Gendler, & J. Hawthorne (Eds.), *The Oxford Handbook of Philosophical Methodology* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199668779.013.10

Lloyd, M. (2008). *The passport: The history of man's most travelled document*. Canterbury: Queen Anne's Fan.

Locke, J. (1988). *Locke: Two Treatises of Government Student edition*. (P. Laslett, Ed.) (Student edition). Cambridge New York Port Melbourne New Delhi Singapore: Cambridge University Press.

Loosemore, T. (2017, June 28). Definition of Digital. Retrieved October 13, 2020, from https://definitionofdigital.com/

Lopez, J. (2021, March 17). Julia Lopez MP Speech to The Investing and Savings Alliance (TISA). Retrieved February 11, 2024, from https://www.gov.uk/government/speeches/julia-lopez-speech-to-the-investing-and-savings-alliance

Lord Ashscroft Polls. (2023). *The State We're In*. Lord Ashcroft Polls. Retrieved from https://lordashcroftpolls.com/wp-content/uploads/2023/09/LORD-ASHCROFT-POLLS-The-State-Were-In-Sept-2023.pdf

Lovett, F. (2018). Republicanism. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Summer 2018). Metaphysics Research Lab, Stanford University. Retrieved from https://plato.stanford.edu/archives/sum2018/entries/republicanism/

LSE. (2005). *The Identity Project: An assessment of the UK Identity Cards Bill and its implications*. London, UK: LSE: Department of Information Systems.

Lucassan, L. (2001). A many-headed monster: The evolution of the passport system in the Netherlands and Germany in the long nineteenth century. In J. Caplan & J. Torpey (Eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World* (pp. 235–255). Princeton, NJ: Princeton University Press.

Lyon, D. (2001). Facing the future: Seeking ethics for everyday surveillance. *Ethics and Information Technology*, 1–12.

Lyon, D (Ed.). (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London: Routledge. https://doi.org/10.4324/9780203994887

Lyon, D. (2006). *Theorizing surveillance: The panopticon and beyond*. Willan Publishing.

Lyon, D. (2009). *Identifying citizens: ID cards as surveillance*. Cambridge, UK: Polity.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Macdonald, C, & Lenihan, R. (2018). Paper Soldiers: The life, death and reincarnation of nineteenth-century military files across the British Empire. *Rethinking History*, *22*(3), 375–402. https://doi.org/10.1080/13642529.2018.1486942

MacKenzie, C. (2008). Relational Autonomy, Normative Authority and Perfectionism. *Journal of Social Philosophy*, *39*(4), 512–533. https://doi.org/10.1111/j.1467-9833.2008.00440.x

Macnish, K. (2015). An Eye for an Eye: Proportionality and Surveillance. *Ethical Theory and Moral Practice*, *18*(3), 529–548. https://doi.org/10.1007/s10677-014-9537-5

Macnish, K. (2017). *The Ethics of Surveillance: An Introduction*. Routledge.

Macnish, K, & Henschke, A (Eds.). (2023). *The Ethics of Surveillance in Times of Emergency*. Oxford University Press. https://doi.org/10.1093/oso/9780192864918.003.0013

Manby, B. (2021). The Sustainable Development Goals and "legal identity for all": "First, do no harm." *World Development*, *139*. https://doi.org/gjmhf7

Manders-Huits, N. (2010). Practical Versus Moral Identities in Identity Management. *Ethics and Information Technology*, *12*(1), 43–55. https://doi.org/10.1007/s10676-010-9216-8

Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*, *25*(2), 185–213. https://doi.org/10.1017/S0003975600004239

Margetts, H. (1999). *Information technology in government: Britain and America*. London ; New York: Routledge.

Margetts, H, & Dunleavy, P. (2013). The Second Wave of Digital-Era Governance: A Quasi-Paradigm for Government on the Web. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *371*(1987), 1–17. https://doi.org/10.1098/rsta.2012.0382

Margetts, H, & Dunleavy, P. (2024). The political economy of digital government: How Silicon Valley firms drove conversion to data science and artificial intelligence in public management. *Public Money & Management*, *0*(0), 1–11. https://doi.org/10.1080/09540962.2024.2389915

Margetts, H, & Naumann, A. (2017). *Government as a Platform: What Can Estonia Show the World?* Oxford Internet Institute.

Mario Lavizzari, MG, Luzio, MD, & Tommasino, C. (2021). The development of digital identity in the Financial Service Industry: From an element that enables digital transactions to a new strategic asset for business. *Journal of Digital Banking*, *6*(1), 57–65.

Marotta-Wurgler, F. (2012). Does Contract Disclosure Matter? *Journal of Institutional and Theoretical Economics*, *168*(1), 1–94. https://doi.org/10.1628/093245612799440122

Marsman, H. (2024). Ethics and Digital Identity. *IDPro Body of Knowledge*, *1*(14), 1–9. https://doi.org/10.55621/idpro.104

Martin, Aaron K. (2012). National Identity Infrastructures: Lessons from the United Kingdom. In M. D. Hercheui, D. Whitehouse, W. McIver, & J. Phahlamohlaka (Eds.), *ICT Critical Infrastructures and Society* (pp. 44–55). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-33332-3_5

Martin, Aaron K, & Whitley, E. (2013). Fixing identity? Biometrics and the tensions of material practices. *Media, Culture & Society*, *35*(1), 52–60. https://doi.org/10.1177/0163443712464558

Martin, Andrew, & Martinovic, I. (2016). Security and Privacy Impacts of a Unique Personal Identifier. *Working Paper Series*, (4), 1–19.

Martin, Aaron, & Taylor, L. (2020). Exclusion and inclusion in identification: Regulation, displacement and data justice. *Information Technology for Development*, *0*(0), 1–17. https://doi.org/10.1080/02681102.2020.1811943

Masiero, S, & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, *31*(6), 903–928. https://doi.org/10.1111/isj.12351

Masiero, S, & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. *Information Technology for Development*, *27*(1), 1–12. https://doi.org/10.1080/02681102.2021.1859669

Masiero, S, & Buddha, C. (2021). Data justice in digital social welfare: A study of the rythu bharosa scheme, 11.

Matt, R. (2018, July 9). The rise and fall of GDS: Lessons for digital government. Retrieved August 14, 2024, from https://www.globalgovernmentforum.com/the-rise-and-fall-of-gds-lessons-for-digital-government/

Mattei, L, Morpurgo, F, Occhipinti, C, Ratto Vaquer, LM, & Vasylieva, T. (2024). Self-Sovereign Identity Model: Ethics and Legal Principles. *Digital Society*, *3*(2), 1–25. https://doi.org/10.1007/s44206-024-00113-2

Mayer-Schonberger, V, & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.

McKenzie, R, Crompton, M, & Wallis, C. (2008). Use Cases for Identity Management in E-Government. *IEEE Security Privacy*, *6*(2), 51–57. https://doi.org/frv22c

Meints, M, & Gasson, M. (2009). High-Tech ID and Emerging Technologies. In K. Rannenberg, D. Royer, & A. Deuker (Eds.), *The future of identity in the information society: Challenges and opportunities* (pp. 129–190). Berlin Heidelberg: Springer.

Microsoft. (2000). Microsoft_2000: Annual Report Letter To Shareholders. Retrieved from https://www.microsoft.com/investor/reports/ar00/lts.htm

Milano, S, Taddeo, M, & Floridi, L. (2020). Recommender systems and their ethical challenges. *AI & SOCIETY*, *35*(4), 957–967. https://doi.org/10.1007/s00146-020-00950-y

Mill, JS. (1900). *Principles of Political Economy*. the colonial press. Retrieved from http://archive.org/details/principlesofpoli0002john

Mill, JS. (1984). *Utilitarianism, On Liberty and Considerations on Representative Government*. (H. B. Acton, Ed.). Dent.

Mill, JS, Bentham, J, Austin, J, & Warnock, M. (2003). *Utilitarianism and On liberty: Including Mill's Essay on Bentham and selections from the writings of Jeremy Bentham and John Austin* (2. ed). Oxford: Blackwell.

Miller, D. (1999). *Principles of Social Justice*. Cambridge, Mass: Harvard University Press.

Mittelstadt, BD, Stahl, BC, & Fairweather, NB. (2015). How to Shape a Better Future? Epistemic Difficulties for Ethical Assessment and Anticipatory Governance of Emerging Technologies. *Ethical Theory and Moral Practice*, *18*(5), 1027–1047. https://doi.org/ggn3cq

Moran, M. (2003). *The British Regulatory State: High Modernism and Hyper-Innovation* (1st ed.). Oxford University Press. Retrieved from https://academic.oup.com/book/2300

Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs.

Morton, B. (2024, July 7). Labour rejects Tony Blair's call for ID cards. *BBC News: Politics*. Retrieved from https://www.bbc.com/news/articles/c87rgj4e0rzo

Mukerji, C. (2011). Jurisdiction, inscription, and state formation: Administrative modernism and knowledge regimes. *Theory and Society*, *40*(3), 223–245. https://doi.org/10.1007/s11186-011-9141-9

Nash, J, & Smith, CH. (2023). Rewiring the Web: The Future of Personal Data. *Demos*. Retrieved from https://demos.co.uk/research/rewiring-the-web-the-future-of-personal-data/

National Audit Office. (2014). *Identity Assurance Programme Briefing Paper*. National Audit Office.

National Audit Office. (2019). *Investigation into Verify*. National Audit Office.

Nayar, PK. (2015). *Citizenship and identity in the age of surveillance*. Delhi: Cambridge University Press.

Needham, C. (2007). *The Reform of Public Services under New Labour: Narratives of Consumerism*. Palgrave Macmillan UK. Retrieved from http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=361594

Neocleous, M. (2007). Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics. *Contemporary Political Theory*, *6*(2), 131–149. https://doi.org/10.1057/palgrave.cpt.9300301

NHS Digital. (2022, September 28). Milestone hit with over 30 million NHS App sign-ups and almost 450K new organ donation decisions. Retrieved March 1, 2024, from https://digital.nhs.uk/news/2022/milestone-hit-with-over-30-million-nhs-app-sign-ups-and-almost-450k-new-organ-donation-decisions

Nick, E. (2011). The Conservative Party and the "Big Society." In C. Holden, M. Kilkey, & G. Ramia (Eds.), *Social Policy Review 23: Analysis and Debate in Social Policy, 2011* (pp. 44–62). Policy Press. https://doi.org/10.1332/policypress/9781847428301.003.0003

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119–158.

Noble, SU. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Nullmeier, F, & Kaufmann, F-X. (2021). Post-War Welfare State Development: The "Golden Age." In D. Béland, S. Leibfried, K. J. Morgan, H. Obinger, & C. Pierson (Eds.), *The Oxford Handbook of the Welfare State* (pp. 93–111). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198828389.013.6

Nussbaum, MC. (2000). *Women and Human Development: The Capabilities Approach*. Cambridge: Cambridge University Press.

Nyst, C, Makin, P, Pannifer, S, & Whitley, E. (2016). Digital Identity: Issue analysis. *Consult Hyperion*.

O'Reilly, T. (2011). Government as a Platform. *Innovations: Technology, Governance, Globalization*, *6*(1), 13–40. https://doi.org/ftv9d4

Ogura, T. (2006). Electronic Government and Surveillance-Oriented Society. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 270–295). Willan Publishing.

OIX. (2021). *ID Inclusion & Data Sets Project Report*. The Open Identity Exchange. Retrieved from https://openidentityexchange.org/networks/87/item.html?id=498

OIX. (2023). OIX - About/Advisory Board. Retrieved September 2, 2024, from https://openidentityexchange.org/advisory-board

One Login Support Team. (2024, April 13). GDS Support Services Request. E-mail.

ONS. (2019, March 4). Exploring the UK's digital divide. Retrieved August 19, 2024, from https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/exploringtheuksdigitaldivide/2019-03-04

ONS. (2022). *Trust in government, UK (2021)*. Office for National Statistics. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/trustingovernmentuk/2022

ONS. (2024, March 1). Trust in government, UK: 2023 — Statistical Bulletin. Retrieved April 21, 2024, from https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/trustingovernmentuk/2023

Oppliger, R. (2003). Microsoft .Net Passport: A security analysis. *Computer*, *36*(7), 29–35. https://doi.org/10.1109/MC.2003.1212687

Oppliger, R. (2004). Microsoft .NET Passport and identity management. *Information Security Technical Report*, *9*(1), 26–34. https://doi.org/10.1016/S1363-4127(04)00013-5

Orgad, L, & Reijers, W. (2021). How to Make the Perfect Citizen? Lessons from China's Social Credit System. *Vanderbilt Journal of International Law*, *54*, 1087–1121.

Orlowski, A. (2015, February 18). Inside GOV.UK: 'Chaos' and 'nightmare' as trendy Cabinet Office wrecked govt websites. *The Register*. Retrieved from https://www.theregister.com/2015/02/18/the_inside_story_of_govuk/

Otjacques, B, Hitzelberger, P, & Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems*, *23*(4), 29–51. https://doi.org/10.2753/MIS0742-1222230403

Palumbo, A. (2004). From Thatcherism to Blairism: Britain's Long March to the Market. *Österreichische Zeitschrift Für Soziologie*, *29*(4), 5–29. https://doi.org/10.1007/s11614-004-0028-0

Pelizza, A, Milan, S, & Lausberg, Y. (2021). Understanding migrants in COVID-19 counting: Rethinking the data-(in)visibility nexus. *Data & Policy*, *3*, 1–18. https://doi.org/10.1017/dap.2021.19

Perez, N. (2020). What are data good for anyway?: A typology of usages of data in contemporary political theory. *Social Theory and Practice*. https://doi.org/ggqtx5

Pettit, P. (1997). *Republicanism: A theory of freedom and government*. Oxford : New York: Clarendon Press ; Oxford University Press.

Pogge, T. (2007). *John Rawls: His Life and Theory of Justice*. (M. Kosch, Trans.). New York: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195136364.001.0001

Pool, I de S. (1983). *Technologies of Freedom*. Harvard University Press.

Posner, EA, & Weyl, EG. (2018). *Radical markets: Uprooting capitalism and democracy for a just society*. Princeton University Press.

POST. (1998). *Electronic Government: Information Technologies and the Citizen*. London: Parliamentary Office of Science and Technology.

Powell, M, & Powell, M (Eds.). (2008). Conclusion: The Blair legacy. In *Modernising the welfare state: The Blair legacy* (pp. 255–274). Policy Press. https://doi.org/10.1332/policypress/9781847420404.003.0015

Price, G. (2008). The benefits and drawbacks of using electronic identities. *Information Security Technical Report*, 9. https://doi.org/10.1016/j.istr.2008.07.002

Prime Minister's Office. (2023, February 7). Making Government Deliver for the British People. Retrieved August 25, 2024, from https://www.gov.uk/government/publications/making-government-deliver-for-the-british-people/making-government-deliver-for-the-british-people-html

Prime Minister's Office. (2024a, July 5). Keir Starmer's first speech as Prime Minister: 5 July 2024. Retrieved August 23, 2024, from https://www.gov.uk/government/speeches/keir-starmers-first-speech-as-prime-minister-5-july-2024

Prime Minister's Office. (2024b, July 17). King's Speech 2024: Background briefing notes. HM Government. Retrieved from https://www.gov.uk/government/publications/kings-speech-2024-background-briefing-notes

Privacy International. (2020, July). The looming disaster of immunity passports and digital identity. Retrieved July 21, 2020, from https://privacyinternational.org/long-read/4074/looming-disaster-immunity-passports-and-digital-identity

Public Accounts Committee. (2013, March 4). House of Commons Uncorrected Transcript of Oral Evidence Hc1024-i: The Government's ICT Savings Initiatives/Improving Government Procurement. House of Commons. Retrieved from https://publications.parliament.uk/pa/cm201213/cmselect/cmpubac/uc1024-i/uc102401.htm

Public Accounts Committee. (2019a). *Government flagship digital identification system failing its users*. UK Parliament. Retrieved from https://committees.parliament.uk/committee/127/public-accounts-committee/news/98272/government-flagship-digital-identification-system-failing-its-users/

Public Accounts Committee. (2019b, May 8). Accessing public services through the Government's Verify digital system inquiry. Retrieved August 15, 2024, from https://committees.parliament.uk/work/3969/accessing-public-services-through-the-governments-verify-digital-system-inquiry/publications/

Public Law Project. (2023). *Public Law Project House of Commons second reading briefing on the Data Protection and Digital Information (No.2) Bill*. Retrieved from https://publiclawproject.org.uk/content/uploads/2023/04/PLP-Briefing-DPDI-Bill-No.2-Second-Reading-Final-1.pdf

Raab, C. (2009). Identity: Difference and Categorization. In I. Kerr, V. M. Steeves, & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, privacy, and identity in a networked society* (pp. 303–318). Oxford University Press.

Raab, C, & Bennett, CJ. (1998). The Distribution of Privacy Risks: Who Needs Protection? *The Information Society*, *14*(4), 263–274. https://doi.org/10.1080/019722498128719

Ramnath, NS, & Assisi, C. (2018). *The Aadhaar Effect: Why the World's Largest Identity Project Matters*. New Delhi, India: Oxford University Press.

Rannenberg, K, Royer, D, & Deuker, A (Eds.). (2009). *The Future of Identity in the Information Society: Challenges and Opportunities*. Berlin Heidelberg: Springer.

Rawls, J. (1951). Outline of a Decision Procedure for Ethics. *The Philosophical Review*, *60*(2), 177–197. https://doi.org/fpn9w7

Rawls, J. (1974). The Independence of Moral Theory. *Proceedings and Addresses of the American Philosophical Association*, *48*, 5–22. https://doi.org/b6skdk

Rawls, J. (2005). *A Theory of Justice* (Original Edition). Cambridge, Mass: Harvard University Press.

Rawls, J. (2020). *A Theory of Justice: Revised Edition*. Harvard University Press. https://doi.org/10.2307/j.ctvkjb25m

Rawls, J, & Kelly, E. (2001). *Justice as fairness: A restatement*. Cambridge, Mass: Harvard University Press.

Raz, J. (2009). *The Morality of Freedom* (Repr). Oxford: Clarendon Press.

Reinecke, C. (2009). Governing Aliens in Times of Upheaval: Immigration Control and Modern State Practice in Early Twentieth-Century Britain, Compared with Prussia. *International Review of Social History*, *54*(1), 39–65. https://doi.org/10.1017/S0020859009000029

Reinecke, J, Arnold, DG, & Palazzo, G. (2016). Qualitative Methods in Business Ethics, Corporate Responsibility, and Sustainability Research. *Business Ethics Quarterly*.

Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview. *Internet Policy Review*, *11*(3). https://doi.org/10.14763/2022.3.1670

Rhodes, RaW. (2000). New Labour's Civil Service: Summing-up Joining-up. *The Political Quarterly*, *71*(2), 151–166. https://doi.org/10.1111/1467-923X.00290

Ricoeur, P. (1994). *Oneself as Another*. (K. Blamey, Trans.). University of Chicago Press.

Ritchie, DG. (1896). *Principles of State Interference* (2nd Edition). Swan Sonnenschein.

Roberts, A. (2015). Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications: Privacy, Data Retention and Domination. *The Modern Law Review*, *78*(3), 535–548. https://doi.org/10.1111/1468-2230.12127

Robertson, N. (2016). *The Co-operative Movement and Communities in Britain, 1914-1960*. Routledge. https://doi.org/10.4324/9781315615035

Rolph, CH. (2004). The English Identity Cards. In C. Watner & W. McElroy (Eds.), *National Identification Systems: Essays in Opposition* (pp. 125–131). McFarland.

Rose, N. (1999). *Powers of Freedom: Reframing Political Thought*. Cambridge University Press.

Rosner, G. (2014, July). *Identity Management Policy and Unlinkability: A Comparative Case Study of the Us and Germany* (Doctoral Thesis). University of Nottingham.

Ruth, L. (2011). The age of responsibility: Social policy and citizenship in the early 21st century. In C. Holden, M. Kilkey, & G. Ramia (Eds.), *Social Policy Review 23: Analysis and Debate in Social Policy, 2011* (pp. 63–84). Policy Press. https://doi.org/10.1332/policypress/9781847428301.003.0004

Saetra, HS. (2021). *Big data's threat to liberty: Surveillance, nudging, and the curation of information* (1st ed.). Waltham: Elsevier.

Sætra, HS. (2019). Freedom under the gaze of Big Brother: Preparing the grounds for a liberal defence of privacy in the era of Big Data. *Technology in Society*, *58*, 101160. https://doi.org/10.1016/j.techsoc.2019.101160

Saltzman, M. (2022, April 20). 50 Most Common Passwords of 2024—Are Yours on the List? Retrieved June 28, 2024, from https://www.rd.com/article/passwords-hackers-guess-first/

Sandel, MJ. (2012). *What money can't buy: The moral limits of markets* (1. publ). London: Allen Lane.

Santo, M. (2016). *House of Lords Library Note: Identity Cards in the UK*. London: House of Lords. Retrieved from https://researchbriefings.files.parliament.uk/documents/LLN-2016-0002/LLN-2016-0002.pdf

Sattarov, F. (2019). *Power and technology: A philosophical and ethical analysis*. Lanham: Rowman & Littlefield.

Savage, M. (1986). The Imposition of Pass Laws on the African Population in South Africa 1916–1984. *African Affairs*, *85*(339), 181–205. https://doi.org/10.1093/oxfordjournals.afraf.a097774

Say, M. (2023, August 29). Post Office to provide face-to-face identity checks for One Login. Retrieved August 29, 2023, from https://www.ukauthority.com/articles/post-office-to-provide-face-to-face-identity-checks-for-one-login/

Say, M. (2024, March 3). The GDS ambition for personalised, proactive services. *UKAuthority*. Retrieved from https://www.ukauthority.com/articles/the-gds-ambition-for-personalised-proactive-services/

Schmidt, D. (2005). *Statistik und Staatlichkeit* (1. Aufl). Wiesbaden: VS Verlag für Sozialwissenschaften.

Schoemaker, E, Baslan, D, Pon, B, & Dell, N. (2020). Identity at the margins: Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development*, *0*(0), 1–24. https://doi.org/gg4t7p

Scott, JC. (1998). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven ; London.

Scott, JC. (2010, September 27). Some Replies on Markets, Languages, and Law. Retrieved August 14, 2024, from https://www.cato-unbound.org/2010/09/27/james-c-scott/some-replies-markets-languages-law

Sedlmeir, J, Smethurst, R, Rieger, A, & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Sen, A. (1983). *Poverty and famines: An essay on entitlement and deprivation*. Oxford: Oxford Univ. Press.

Sen, A. (1985). Well-Being, Agency and Freedom: The Dewey Lectures 1984. *The Journal of Philosophy*, *82*(4), 169–221. https://doi.org/10.2307/2026184

Sen, A. (1995). Equality of What? In A. Sen (Ed.), *Inequality Reexamined* (p. 0). Oxford University Press. https://doi.org/10.1093/0198289286.003.0002

Sen, A. (1999). *Development as Freedom*. Oxford: Oxford University Press.

Sengoopta, C. (2004). *Imprint of the Raj: How fingerprinting was born in colonial India*. London: Pan Books.

Shapps, G, & Williams, K. (2021). *Great British Railways: The Williams-Shapps Plan for Rail*. Department for Transport. Retrieved from https://www.gov.uk/government/publications/great-british-railways-williams-shapps-plan-for-rail

Skinner, Q. (2008). *Hobbes and Republican Liberty* (Illustrated Edition). Cambridge, UK ; New York: Cambridge University Press.

Slow, O. (2023, July 1). No free lunch for nationalisation of water firm says Lord Howard. *BBC News: UK*. Retrieved from https://www.bbc.com/news/uk-66074484

Smith, CH. (2020). Corporatised Identities ≠ Digital Identities: Algorithmic Filtering on Social Media and the Commercialisation of Presentations of Self. In C. Burr & L. Floridi (Eds.), *Ethics of Digital Well-being: A Multidisciplinary Approach* (pp. 55–80).

Smith, CH. (2023). Digitising reflective equilibrium. *Ethics and Information Technology*, *25*(3). https://doi.org/10.1007/s10676-023-09722-w

Smith, JEH. (2022). *The internet is not what you think it is: A history, a philosophy, a warning*. Princeton: Princeton University Press.

Smith, PT. (2020). A Neo-Republican Theory of Just State Surveillance. *Moral Philosophy and Politics*, *7*(1), 49–71. https://doi.org/ghcgzr

Smyth, C, & Sellman, M. (2024, August 26). Government-backed "digital IDs" to let people open bank accounts. *The Times*. Retrieved from https://www.thetimes.com/uk/politics/article/government-backed-digital-ids-will-provide-trust-mark-for-paying-taxes-808gxzww9

Smyth, SM. (2019). *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control* (1st ed.). Routledge. https://doi.org/10.4324/9780429022326

Søe, SO, & Mai, J-E. (2022). Data identity: Privacy and the construction of self. *Synthese*, *200*(6), 1–22. https://doi.org/10.1007/s11229-022-03968-5

Solove, Daniel J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York, NY: NYU Press.

Solove, Daniel J. (2008). Privacy: A Concept in Disarray. In *Understanding Privacy* (pp. 1–11). Harvard University Press.

Sparks, J, & Jayaram, A. (2022). Rule by Automation: How Automated Decision Systems Promote Freedom and Equality. *Moral Philosophy and Politics*, *9*(2), 201–218. https://doi.org/10.1515/mopp-2020-0066

Spence, A. (2019, September 10). Boris Johnson's Secret Plan To Gather "Targeted And Personalised" Data Before Brexit. Retrieved November 5, 2019, from https://www.buzzfeed.com/alexspence/boris-johnson-dominic-cummings-voter-data

Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology*, *18*(1), 33–39. https://doi.org/10.1007/s10676-016-9392-2

Stalla-Bourdillon, S, Pearce, H, & Tsakalakis, N. (2018). The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify. *Computer Law & Security Review*, *34*(4), 784–805. https://doi.org/10.1016/j.clsr.2018.05.012

Strong, C. (2010). Theoretical and practical problems with wide reflective equilibrium in bioethics. *Theoretical Medicine and Bioethics*, *31*(2), 123–140. https://doi.org/dvn6qz

Sullivan, C. (2007). Conceptualising Identity. *International Review of Law, Computers & Technology*, *21*(3), 237–261. https://doi.org/10.1080/13600860701701447

Sullivan, C. (2011). *Digital Identity: An Emergent Legal Concept*. University of Adelaide Press.

Susskind, J. (2020). *Future politics: Living together in a world transformed by tech.* Oxford University Press.

Susskind, J. (2022). *The digital republic: On freedom and democracy in the 21st century*. Bloomsbury. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=3292499

Swift, A, & White, S. (2008). Political Theory, Social Science, and Real Politics. In D. Leopold & M. Stears (Eds.), *Political theory: Methods and approaches*. Oxford ; New York: Oxford University Press.

Szreter, S. (2007). The Right of Registration: Development, Identity Registration, and Social Security—A Historical Perspective. *World Development*, *35*(1), 67–86. https://doi.org/bcqrc2

Taddeo, M. (2019). The Civic Role of Online Service Providers. *Minds and Machines*, *29*(1), 1–7. https://doi.org/10.1007/s11023-019-09495-6

Tavani, HT. (2008). Informational Privacy: Concepts, Theories, and Controversies. In *The Handbook of Information and Computer Ethics* (pp. 131–164). John Wiley & Sons, Ltd. https://doi.org/10.1002/9780470281819.ch6

Taylor, AJP. (1965). *English History, 1914-1945*. Oxford University Press.

Taylor, C (Ed.). (1985). What's wrong with negative liberty. In *Philosophical Papers: Volume 2: Philosophy and the Human Sciences* (Vol. 2, pp. 211–229). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139173490.009

Taylor, JA, Lips, AMB, & Organ, J. (2009). Identification practices in government: Citizen surveillance and the quest for public service improvement. *Identity in the Information Society*, *1*(1), 135–154. https://doi.org/fh2pvk

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2), 1–14. https://doi.org/10.1177/2053951717736335

Taylor, M. (2021, July 13). A single sign-on and digital identity solution for government - Government Digital Service. Retrieved February 11, 2024, from https://gds.blog.gov.uk/2021/07/13/a-single-sign-on-and-digital-identity-solution-for-government/

Tersman, F. (2018). Recent work on reflective equilibrium and method in ethics. *Philosophy Compass*, *13*(6), 1–10. https://doi.org/gc2fdd

The Editorial Board. (2023, June 30). England's ill-fated experiment with privatising water. *Financial Times: The FT View*. Retrieved from https://www.ft.com/content/fec133e3-f818-4a3c-8f96-079c0649bbe8

The Guardian. (2021, March 9). The Guardian view on voting rights: Don't import US-style suppression. *The Guardian: Opinion*. Retrieved from https://www.theguardian.com/commentisfree/2021/mar/09/the-guardian-view-on-voting-rights-dont-import-us-style-suppression

Theodorou, Y. (2022). *On the Road to Digital-ID Success in Africa: Leveraging Global Trends*. London, UK: Tony Blair Institute for Global Change. Retrieved from https://institute.global/policy/road-digital-id-success-africa-leveraging-global-trends

Thompson, S. (2008). Separating the Sheep from the Goats: The United Kingdom's National Registration Programme and Social Sorting in the Pre-Electronic Era. In C. J. Bennett & D. Lyon (Eds.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (pp. 145–162). London, UK: Routledge.

Tocqueville, A de. (2004). *Democracy in America*. (O. Zunz, Ed., A. Goldhammer, Trans.) (2. print). New York: Library of America.

Tony Blair Institute. (2019). *Response to DCMS-GDS Call for Evidence on Digital Identity*. London, UK: Tony Blair Institute for Global Change. Retrieved from https://institute.global/sites/default/files/inline-files/TBIGC%20Response%20to%20DCMS-GDS%20Call%20for%20Evidence%20on%20Digital%20Identity.pdf

Torpey, J. (2000). *The Invention of the Passport: Surveillance, Citizenship and the State*. Cambridge, UK: Cambridge University Press.

Torpey, J. (2001). The Great War and the Birth of the Modern Passport System. In J. Caplan & J. Torpey (Eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton, NJ: Princeton University Press.

Trauth-Goik, A, & Bernot, A. (2021). Decentralising Data Collection and Centralising Information in the People's Republic of China: Decentralise, Manage, and Service Reforms. *Surveillance & Society*, *19*(4), 518–553. https://doi.org/10.24908/ss.v19i4.14371

Tréguer, F. (2019). Seeing like Big Tech: Security assemblages, technology, and the future of state bureaucracy. In *Data Politics*. Routledge.

Trendall, S. (2023, June 26). HMRC and DWP to start using One Login within the next year. Retrieved March 31, 2024, from https://www.civilserviceworld.com/professions/article/hmrc-and-dwp-to-start-using-one-login-within-the-next-year

Trendall, S. (2024a, January 17). One Login: GDS signs £10m deal for fraud-prevention system. Retrieved March 18, 2024, from https://www.publictechnology.net/2024/01/17/defence-and-security/one-login-gds-signs-10m-deal-for-fraud-prevention-system/

Trendall, S. (2024b, March 27). Government trebles number of services using One Login. Retrieved March 31, 2024, from https://www.civilserviceworld.com/professions/article/one-login-government-trebles-number-services

Trikanad, S. (2020). *Estonia's E-Identity Programme*. India: The Centre for Internet and Society.

Tsakalakis, N, O'Hara, K, & Stalla-Bourdillon, S. (2016). Identity assurance in the UK: Technical implementation and legal implications under the eIDAS regulation. In *Proceedings of the 8th ACM Conference on Web Science - WebSci '16* (pp. 55–65). Hannover, Germany: ACM Press. https://doi.org/10.1145/2908131.2908152

Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. Simon & Schuster.

Turley, L. (2020). *Trustworthy Digital Infrastructure for Identity Systems: The Global Imperative*. Alan Turing Institute. Retrieved from https://www.turing.ac.uk/sites/default/files/2020-12/alan_turing_digital_identities_2020.pdf

Vallor, S. (2016). *Technology and the virtues: A philosophical guide to a future worth wanting*. New York, NY: Oxford University Press.

Vallor, S. (2022). Introducing the Philosophy of Technology. In S. Vallor, S. Vallor (Ed.), *The Oxford Handbook of Philosophy of Technology* (pp. xviii–16). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190851187.013.1

van de Poel, I. (2016). A Coherentist View on the Relation Between Social Acceptance and Moral Acceptability of Technology. In M. Franssen, P. E. Vermaas, P. Kroes, & A. W. M. Meijers (Eds.), *Philosophy of Technology after the Empirical Turn* (Vol. 23, pp. 177–193). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-33717-3_11

van der Burg, W, & van Willigenburg, T. (1998). Introduction. In *Reflective Equilibrium: Essays in Honour of Robert Heeger* (pp. 1–25). Dordrecht Boston London: Kluwer Academic Publishers.

Véliz, C. (2021). *Privacy is power: Why and how you should take back control of your data*. London: Corgi Books.

Véliz, C. (2024a). Privacy in the Twenty-First Century. In C. Véliz (Ed.), *The Ethics of Privacy and Surveillance*. Oxford University Press. https://doi.org/10.1093/oso/9780198870173.003.0014

Véliz, C. (2024b). Privacy vs Surveillance. In C. Véliz (Ed.), *The Ethics of Privacy and Surveillance*. Oxford University Press. https://doi.org/10.1093/oso/9780198870173.003.0010

Véliz, C. (2024c). *The Ethics of Privacy and Surveillance*. Oxford University Press. https://doi.org/10.1093/oso/9780198870173.001.0001

Véliz, C. (2024d). The Value of Surveillance. In C. Véliz (Ed.), *The Ethics of Privacy and Surveillance*. Oxford University Press. https://doi.org/10.1093/oso/9780198870173.003.0009

Verbeek, P-P. (2011). *Moralizing Technology: Understanding and Designing the Morality of Things*. https://doi.org/10.7208/chicago/9780226852904.001.0001

Vidler, E, & Clarke, J. (2005). Creating Citizen-Consumers: New Labour and the Remaking of Public Services. *Public Policy and Administration*, *20*(2), 19–37. https://doi.org/10.1177/095207670502000202

Voinea, CF, Neumann, M, & Troitzsch, KG. (2023). The State and the Citizen: Overview of a complex relationship from a paradigmatic perspective. *Quality & Quantity*, *57*(1), 1–17. https://doi.org/10.1007/s11135-022-01474-x

Wachter, S. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer Law & Security Review*. https://doi.org/ghdrt4

Wachter, S. (2019). Affinity Profiling and Discrimination by Association in Online Behavioural Advertising [Draft]. *Berkeley Technology Law Journal*. Retrieved from https://papers.ssrn.com/abstract=3388639

Wachter, S, & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2019*(2), 1–126. Retrieved from https://papers.ssrn.com/abstract=3248829

Walden, K. (2013). In defense of reflective equilibrium. *Philosophical Studies*, *166*(2), 243–256. https://doi.org/10.1007/s11098-012-0025-2

Waldron, J. (2017). *One another's equals: The basis of human equality*. Cambridge, Massachusetts: The Belknap Press of Harvard University Press.

Walzer, M. (2010). *Spheres of justice: A defense of pluralism and equality*. New York: Basic Books.

Warren, A, & Mavroudi, E. (2011). Managing Surveillance? The Impact of Biometric Residence Permits on UK Migrants. *Journal of Ethnic and Migration Studies*, *37*(9), 1495–1511. https://doi.org/10.1080/1369183X.2011.623624

Watner, C. (2004). Why I Oppose Government Enumeration. In C. Watner & W. McElroy (Eds.), *National Identification Systems: Essays in Opposition* (pp. 248–254). McFarland. Retrieved from https://books.google.com?id=ArTIEHDqvP8C

Watner, C, & McElroy, W (Eds.). (2004). *National Identification Systems: Essays in Opposition*. McFarland.

Webber, F. (2022). *Citizenship: From Right to Privilege*. The Institute of Race Relations. Retrieved from https://irr.org.uk/product/citizenship-from-right-to-privilege/

Weber, M. (1978). *Economy and Society: An Outline of Interpretive Sociology*. Berkeley, CA: University of California Press.

Webster, F. (2014). *Theories of the Information Society*. Routledge.

West, SM. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Wheeler, C, & Pogrund, G. (2024, July 7). Tony Blair's warning to Keir Starmer on migration. *The Times*. Retrieved from https://www.thetimes.com/uk/politics/article/blair-warns-starmer-on-migration-without-rules-we-get-prejudices-7rj7skdmn

Whitley, E. (2016). GOV.UK Verify: A federated, privacy focussed identity assurance scheme. *Privacy, Laws & Business: International Report*, (142), 22–24.

Whitley, E. (2018). *Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach*. Washington, D.C.: Center for Global Development.

Whitley, EA, & Hosein, G. (2010). *Global challenges for identity policies*. Basingstoke, Hampshire ; New York: Palgrave Macmillan.

Whitley, E, & Hosein, G. (2010). Global Identity Policies and Technology: Do we Understand the Question?: Global Identity Policies. *Global Policy*, *1*(2), 209–215. https://doi.org/10.1111/j.1758-5899.2010.00028.x

Whitley, E, Martin, AK, & Hosein, G. (2014). From surveillance-by-design to privacy-by-design: Evolving identity policy in the United Kingdom. In K. Boersma, R. van Brakel, C. Fonio, & P. Wagenaar (Eds.), *Histories of state surveillance in Europe and beyond* (First Edition). New York: Routledge, Taylor & Francis Group.

Whittaker, F. (2024, May 9). Benefit fraud squad snoops on pupil data under secret deal. *Schools Week*. Retrieved from https://schoolsweek.co.uk/revealed-secret-deal-to-let-benefit-fraud-squad-snoop-on-pupil-data/

Widdershoven, GAM. (2007). How to combine hermeneutics and Wide Reflective Equilibrium?: A comment on M. Ebbesen and B. Pedersen, How to formulate normative ethical principles by use of empirical investigations within biomedicine. *Medicine, Health Care and Philosophy*, *10*(1), 49–52. https://doi.org/d2crz3

Wilcox, M. (2023, February 18). Hundreds march through Oxford in traffic protest turned "anti-globalist" demo. Retrieved September 10, 2024, from https://cherwell.org/2023/02/18/hundreds-march-through-oxford-in-traffic-protest-turned-anti-globalist-demo/

Willars, E. (2019). Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK (White Paper). Retrieved from https://openidentityexchange.org/wp-content/uploads/2019/10/Establishing-a-Trusted-Interoperable-Digital-Identity-Ecosystem-in-the-UK-White-Paper-Oct-2019.pdf

Williams, B. (2021). The "New Right" and its legacy for British conservatism. *Journal of Political Ideologies*, 1–24. https://doi.org/10.1080/13569317.2021.1979139

Williams, W, Great Britain, & Home Office. (2020). *Windrush Lessons Learned Review: Independent review*.

Wills, D. (2008). The United Kingdom Identity Card Scheme: Shifting Motivations, Static Technologies. In C. J. Bennett & D. Lyon (Eds.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (pp. 163–179). London, UK: Routledge.

Wilson, J, Webster, A, & Vorberg-Rugh, R. (2013). The Co-operative Movement in Britain: From Crisis to "Renaissance," 1950–2010. *Enterprise & Society*, *14*(2), 271–302. https://doi.org/10.1093/es/khs076

Wilson, S. (2011). Identities Evolve: Why Federated Identity is Easier Said than Done. *SSRN Electronic Journal*. https://doi.org/gkgg7f

Wilson, S. (2022a). How to Create an Infostructure to Protect Data as a Utility. *Australian Quarterly*, 32–40.

Wilson, S. (2022b). *What will we learn from the Market Failure of Digital Identity?* Presented at the Identiverse 2022, Denver, Colorado. Retrieved from https://lockstep.com.au/wp-content/uploads/2022/07/Steve-Wilson-Identiverse-2022-Market-Failure-0.6-HANDOUTS.pdf

Wilson, Y, & Hingnikar, A. (2019). *Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-5095-2

Windley, PJ. (2005). *Digital Identity*. Sebastopol: O'Reilly Media, Inc.

Winner, L. (1997). Cyberlibertarian Myths and the Prospects for Community. *Computers and Society*, *27*(3), 14–19.

Wolff, J. (2011). *Ethics and public policy: A philosophical inquiry*. Milton Park, Abingdon, Oxon ; New York: Routledge.

Wolff, J. (2015). Political Philosophy and the Real World of the Welfare State. *Journal of Applied Philosophy*, *32*(4), 360–372. https://doi.org/10.1111/japp.12125

Wolff, J. (2018). Method in philosophy and public policy: Applied philosophy versus engaged philosophy. In *The Routledge Handbook of Ethics and Public Policy*. Routledge.

Wolff, J. (2020). Public Reflective Disequilibrium. *Australasian Philosophical Review*, *4*(1), 45–50. https://doi.org/10.1080/24740500.2021.1876413

Wolff, J, & de-Shalit, A. (2007). *Disadvantage*. Oxford University Press. Retrieved from https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199278268.001.0001/acprof-9780199278268

Wolff, J, & de-Shalit, A. (Eds.). (2024). *City of equals*. New York: Oxford University Press. Retrieved from 10.1093/oso/9780198894735.001.0001

Yadron, D. (2014, May 21). Man Behind the First Computer Password: It's Become a Nightmare. *Wall Street Journal: Digits*. Retrieved from http://blogs.wsj.com/digits/2014/05/21/the-man-behind-the-first-computer-password-its-become-a-nightmare/

Yeung, K. (2017). "Hypernudge": Big Data as a mode of regulation by design. *Information, Communication & Society*, *20*(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505–523. https://doi.org/10.1111/rego.12158

YouGov. (2010). YouGov/The Sun Survey Results [Data set]. Retrieved from https://d3nkl3psvxxpe9.cloudfront.net/documents/YG-Archives-Pol-Sun-coalition-160810.pdf

Young, IM. (2001). Equality of Whom? Social Groups and Judgments of Injustice. *Journal of Political Philosophy*, *9*(1), 1–18. https://doi.org/10.1111/1467-9760.00115

Zapata-Barrero, R. (2018). Applied Political Theory and Qualitative Research in Migration Studies. In R. Zapata-Barrero & E. Yalaz (Eds.), *Qualitative Research in European Migration Studies* (pp. 75–92). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-76861-8_5

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

Zuckerman, E. (2020). *The Case for Digital Public Infrastructure*. Knight First Amendment Institute. Retrieved from https://knightcolumbia.org/content/the-case-for-digital-public-infrastructure