

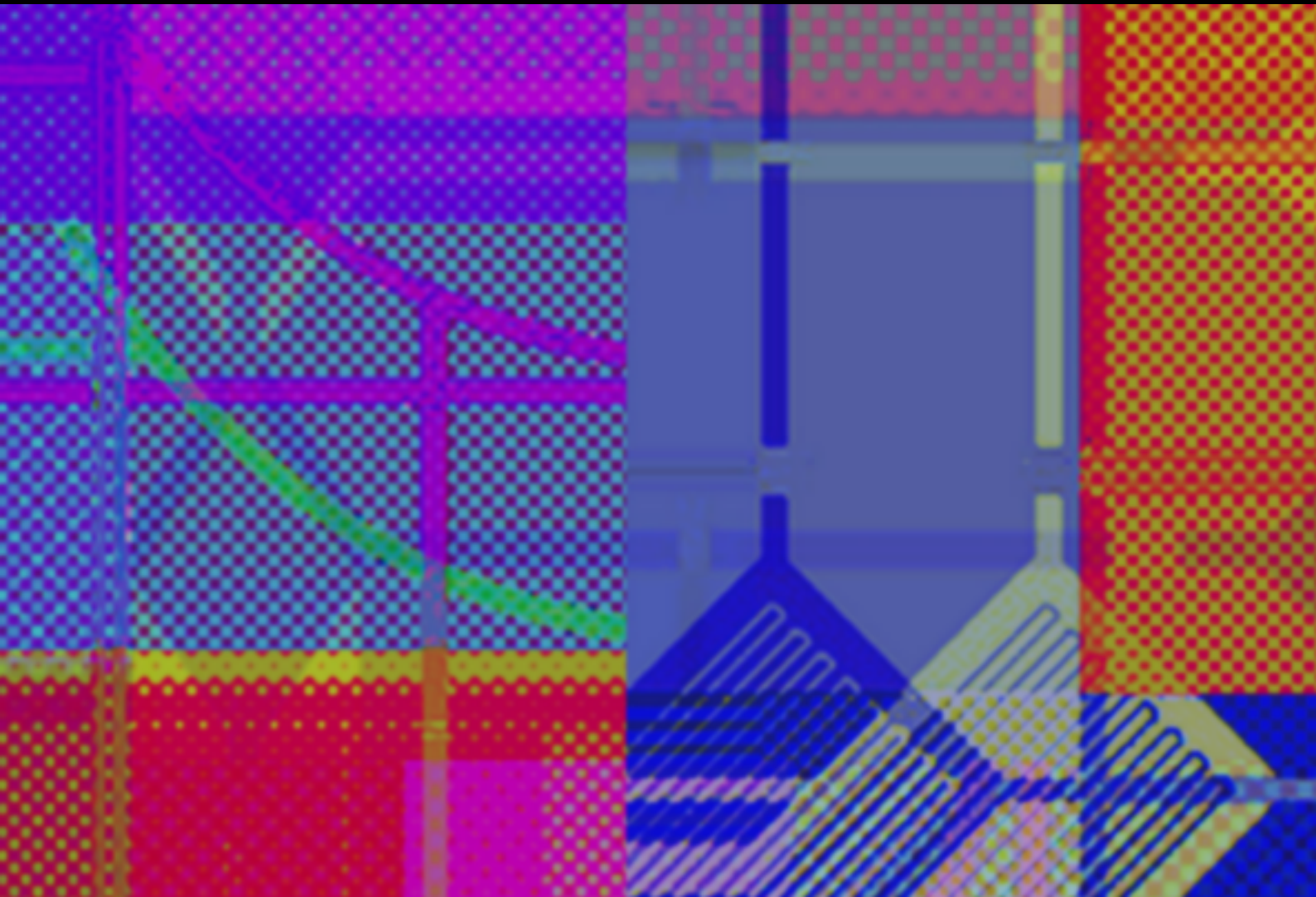


REPORT

TECH GIANTS AND GIANT SLAYERS:

THE CASE FOR DIGITAL SOVEREIGNTY & THE DIGITAL COMMONS

April 2026



ABOUT OPEN RIGHTS GROUP

Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. We work for a world where technology supports justice, rights and freedoms to prevail over powerful monopolistic interests; and neither states nor corporations use digital technology to restrict, monitor or control people.

ABOUT THIS REPORT

Report written by Jim Killock, with contributions from Megan Kirkwood, Terence Eden, Wendy Grossman, Simon Phipps, James Baker, Mariano delli Santi, and Pam Cowburn.

Published in April 2026 by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. Space4, 113-115 Fonthill Road, London N4 3HH.

Published under a Creative Commons Attribution Sharealike licence (CC BY-SA 4.0).



Graphic showing the UK Government systems thinking cycle, in *Systems thinking and UK Digital Sovereignty* from *An introductory systems thinking toolkit for civil servants* and used under the Open Government Licence (OGL) v 3.0.

CONTENTS

FOREWORD.....	7
LORD TIM CLEMENT-JONES CBE.....	8
SIÂN BERRY MP.....	10
CLIVE LEWIS MP.....	12
EXECUTIVE SUMMARY.....	15
RECLAIMING DIGITAL SOVEREIGNTY.....	16
THE HIGH COST OF DIGITAL DEPENDENCY.....	16
THE UK'S CURRENT POSITION:.....	17
DIGITAL SOVEREIGNTY REDUCES COSTS AND GROWS THE DIGITAL ECONOMY.....	17
THE OPPORTUNITY OF THE DIGITAL COMMONS.....	18
THE WAY FORWARD: A ROADMAP TO DIGITAL SOVEREIGNTY.....	19
KEY RECOMMENDATIONS FOR THE UK GOVERNMENT.....	19
INTRODUCTION.....	21
PART I THE DIGITAL SOVEREIGNTY CHALLENGE.....	25
DEFINING DIGITAL SOVEREIGNTY.....	26
CREATING TECH DEPENDENCY.....	28
COMPETITION IS FOR LOSERS.....	28
VENDOR LOCK-IN AT GOVERNMENT.....	29
CONSULTANCY AND AUDITORS.....	30
CLOUD AND AI LOCK-IN.....	32

LOBBYING AND ASTROTURFING.....	32
TRADE AGREEMENTS.....	33
REMOVING THE RIGHT TO REPAIR AND PREVENTING AI TRANSPARENCY.....	34
CHIPS AND DEVICES.....	35

RISKS FROM BUSINESS AS USUAL..... 36

LEGAL RISKS.....	36
US POWERS OF ACCESS.....	36
US POWERS OF SANCTION.....	36
CHINESE POWERS TO DIRECT TECH COMPANIES.....	37
ECONOMIC DEPENDENCY AND EXTRACTION.....	38
IMPACT OF UK TECH COMPANIES BEING SOLD TO TECH GIANTS.....	39
SECURITY RISKS.....	40
POLICY RISKS.....	41
VENDOR-LED POLICY MAKING AND TECH SOLUTIONISM.....	41
ONLINE POLITICAL DISTORTION.....	42

APPROACHES TO DELIVERING SOVEREIGNTY..... 43

BUY PROPRIETARY BRITISH.....	43
SOVEREIGN CLOUD.....	44
IN-HOUSE SOFTWARE.....	44
THE DIGITAL COMMONS: OPEN TECHNOLOGIES.....	44
EUROPEAN AND INTERNATIONAL COLLABORATION.....	45

PART II CURRENT UK POLICY POSITION..... 47

THE GROWTH AGENDA..... 49

COMPETITION POLICY.....	50
STRATEGIC MARKET STATUS AND EX-ANTE OBLIGATIONS.....	50
COMPETITION AND APPEALS TRIBUNAL.....	51
MERGERS AND ACQUISITIONS.....	52
DATA PROTECTION.....	53
SOCIAL MEDIA POLICY.....	53

UK SPENDING ON DIGITAL TECHNOLOGIES..... 54

VENDOR LOCK-IN.....	55
UK AND CLOUD SUPPLIERS.....	57
UK STRATEGIC SUPPLIERS.....	58

WHY IT PROCUREMENT FAILS IN THE UK.....	59
GOVERNMENT DIGITAL SERVICE.....	59
NHS AND PALANTIR, OPENSANELY AND OPENEHR.....	60
WHY IN-SOURCING AND GDS HAVE STRUGGLED.....	60
MODERN DIGITAL GOVERNMENT AND THE COMMERCIAL DIGITAL CENTRE OF EXCELLENCE.....	61
AI PROCUREMENT.....	62
DIGITAL SOVEREIGNTY BEYOND WHITEHALL.....	63
LOCAL GOVERNMENT.....	63
WALES AND SCOTLAND.....	64
THE OPEN SOURCE ECOSYSTEM IN THE UK.....	65
SYSTEMS THINKING AND UK DIGITAL SOVEREIGNTY.....	66
PART III BEYOND THE UK.....	70
LEADING THROUGH STRATEGY, DELIVERY THROUGH DEDICATED INSTITUTIONS....	72
BUILDING AI OUTSIDE OF THE US.....	73
PURSUING AI GROWTH THROUGH OPEN SOURCE.....	73
CLOUD IN EUROPE.....	74
EUROPE AND TECH SECTOR GROWTH.....	76
OPEN SOURCE PRODUCTIVITY AND DESKTOPS.....	76
IDENTITY AND DATA EXCHANGE SYSTEMS.....	78
DIGITAL PAYMENTS.....	79
HEALTH AND SOCIAL SYSTEMS.....	80
EDUCATIONAL TECHNOLOGY.....	80
PROCUREMENT SOFTWARE.....	83
COMMUNITY ENGAGEMENT.....	83
INTERNATIONAL COLLABORATION.....	84

RISC-V: OPEN CHIP DESIGN.....	85
STRENGTHENING OPEN SOURCE.....	85
DEMOCRATIC DISCOURSE AND SOCIAL MEDIA REGULATION.....	86
ONLINE HARMS IN EUROPE.....	86
TACKLING PLATFORM POWER THROUGH EU COMPETITION LAW.....	87
ADDRESSING ONLINE HARMS THROUGH COMPETITION LAW.....	87
PART IV RECOMMENDATIONS FOR A DIGITAL SOVEREIGNTY STRATEGY.....	90
WHERE TO START.....	91
REGULATORY AND ECONOMIC ALIGNMENT WITH EUROPE, OPEN INNOVATION WITH THE US.....	92
GIANTS AND GIANT SLAYERS.....	92
DIGITAL LEADERSHIP.....	93
PROTECTING DEMOCRACY.....	94
A ROADMAP FOR DIGITAL SOVEREIGNTY.....	95
APPENDIX I UK TECH COMPANIES SOLD OVERSEAS.....	101
APPENDIX II SECURITY RISKS, OPEN VS CLOSED TECH.....	105
APPENDIX III SOVEREIGNTY RISK MANAGEMENT.....	107
APPENDIX IV UK TECH STRATEGIC SUPPLIERS.....	111
REFERENCES.....	117

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

FOREWORD

LORD TIM CLEMENT-JONES CBE

Digital Sovereignty has moved from policy seminars to front-page news with stunning speed. When Microsoft shut down the International Criminal Court (ICC) prosecutor's email following a US Executive Order, European governments were forced to confront an uncomfortable truth: we have built critical state infrastructure on foundations we do not control.

The UK faces this dilemma acutely. Scottish police recently discovered their data flows through Microsoft servers in over a hundred countries via "follow the sun" support – accessible to foreign jurisdictions without UK oversight. When asked why they wouldn't guarantee data sovereignty, Microsoft's response was telling: "no one else had asked". This is not about technical capability. It is about political will.

We have what this timely paper describes as a "sovereignty paradox". The Government has announced significant investment to make Britain an AI superpower, yet nearly every pound flows to US hyper-scalers whose terms of service override our laws, whose algorithms remain opaque, and whose dominance creates vendor lock-in that both drains the public purse and stunts our own tech sector.

Throughout the Technology Prosperity Deal negotiations we have been tested over whether Britain retains genuine sovereignty or accepts the status of digital colony. We are facing pressure to abandon our digital services tax, and water down our Online Safety Act in exchange for infrastructure investment that would likely materialise anyway. In my view, the right to tax digital services fairly and regulate harmful content are not negotiating chips they should be red lines.

Yet sovereignty is not about isolation. We cannot be entirely self-sufficient. This essential paper demonstrates that the path forward lies not in isolation, but in strategic autonomy built on Open Source and Open Standards. By adopting 'Public Code for Public Money,' we can ensure that software running our critical infrastructure is transparent, auditable, and genuinely under public control.

The contrast with our European neighbours is stark. Germany has established ZenDiS, its Centre for Digital Sovereignty (ZenDis). France invests heavily in Mistral AI and has secured genuine control over government systems.

TECH GIANTS AND GIANT SLAYERS

Meanwhile, the UK risks being caught between American commercial dominance and European regulatory coordination, benefiting from neither alliance.

What gives me hope is the evidence assembled here that alternative approaches work. The economic case is overwhelming: open source generates £4 for every £1 invested and has created 2-3% of global GDP. France's Open Source preference has driven 9-18% annual growth in tech start-ups. The sovereignty case is equally clear: when you control the code, you control your destiny.

The public understands this instinctively. Focaldata research shows that while few voters could define 'Digital Sovereignty', the underlying choices already matter more to voting behaviour than migration, climate, or even the NHS. Messages about keeping NHS data under British jurisdiction resonate powerfully across all political divides.

This paper provides both the rigorous analysis and practical roadmap we urgently need. It exposes the true costs of our current dependencies and charts a course toward responsible sovereignty—one that balances innovation with resilience, economic opportunity with democratic accountability.

The question now is whether we have the political courage to act. Every procurement decision that embeds foreign dependency, every compromise of sovereignty in the name of convenience, accumulates into strategic vulnerability. The goal of responsible sovereign AI is within reach, but only if we pursue it with both ambition and wisdom.

I commend this paper to anyone who believes that Britain's digital future should be decided in Westminster, not in Silicon Valley.

Lord Clement-Jones CBE,

Lib Dem DSIT Spokesperson in the House of Lords

SIÂN BERRY MP

The need for this report and the actions it recommends could not be more urgent or more serious.

Across the globe, democratic institutions are creaking, with leaders with closer links to billionaires than the people who cast their votes to elect them, ripping up the rules of global order and causing fear and destabilisation.

Without fanfare or sufficient scrutiny, an excessive concentration of tech giants have become responsible for the UK's most critical infrastructure and democratic functions.

And with tariffs and threats being freely deployed by the US President in haste and anger, against allies and foes alike, the very real risk of exposure to an external 'kill switch' for the technology our public services rely upon is looming large.

Pass 'GO', collect £330 million and a trove of our citizens' personal data, and no questions will be asked. It is clearer than ever that here in the UK, there has been nothing strategic or resilient in the practice of successive Governments handing over billions in 'strategic supplier' technology contracts to a small group of companies based in countries that may not have our best interests at heart.

The work ORG has done in promoting open standards and open source technology for years has not always needed to focus on the risks of nefarious actors, however. That is because in purely business and technical terms, these have also been bad decisions.

The closed systems and proprietary software of these companies keep us locked in, not just to the risks of service withdrawal, sanctions or commercial failure. Interoperability, and the chance to shift suppliers without serious technical drag are at odds with the business models of these companies.

And some of the practices of these not-so-friendly giants we rely on sit very uncomfortably with the ethics and values our country holds dear. For example, I have watched in horror as Palantir has crafted data-analytics software to facilitate ICE's fascist deportations, sharing data between government departments to surveil and track migrants. While its CEO, Alex Karp is free to joke

TECH GIANTS AND GIANT SLAYERS

about its mission, saying chillingly in 2025: “Palantir is here to disrupt... and, when it’s necessary, to scare our enemies and, on occasion, kill them.”

Yet thanks to the hold these giant companies have had on government procurement decisions, Palantir’s hand is now set to be gripped around the neck of our beloved NHS.

And it is not as if we even get better products this way. Weakened competition and vendor lock-in has meant the functionality of the digital systems we are currently tied to is so poor they are a running joke in conversations across the land.

This day-to-day technology, for people who need to pay taxes, claim benefits or access the NHS, lets down far too many of the constituents I see in my surgeries, but it could all be made user-friendly, accessible and functional with a new approach that properly puts users before profits. A ‘Public Code for Public Money’ policy could mean public sector apps, online forms and admin screens actually made by and for the people who use them every day.

Our political leaders must heed the risks, and the important recommendations here must now be seen by them as both a safer option and a truly exciting chance to develop better public services, as well as the UK’s own talented technology sector.

The Government would be reckless to ignore this report and fail to tackle Digital Sovereignty for a moment longer.

CLIVE LEWIS MP

Two centuries ago, a director of the British East India Company offered a strikingly candid description of how empire worked. The Company's system, he told Parliament, acted, "like a sponge, drawing up all the good things from the banks of the Ganges and squeezing them down on the banks of the Thames". It was an unusually honest admission of how power flows through infrastructure. Control the system through which value moves, and the value – and the power – will follow.

History does not repeat itself neatly. But it rhymes. Today we would be foolish to ignore the echo.

The question this report addresses is simple but profound: who controls the infrastructure on which modern societies depend? Cloud computing, data systems, artificial intelligence (AI), software platforms and algorithmic networks are no longer peripheral technologies. They are the operating system of modern states, economies and democracies. Yet the UK, like many countries, increasingly relies on a handful of global technology firms to build, operate and maintain them – firms that answer not to democratic institutions but to their shareholders and, in some cases, to foreign governments.

For some time I have been concerned about the direction of travel. We are witnessing a structural shift in the balance of power between states and large technology corporations. Critical infrastructure that once sat within democratic oversight is now increasingly mediated through private platforms and proprietary systems. The implications for sovereignty, accountability and economic resilience are serious.

The report identifies several connected dangers. The first is corporate capture of state infrastructure: when essential systems are designed, owned and operated by private actors, the state's ability to shape its own policy environment narrows. The second is dependency on oligopolies, where vendor lock-in, proprietary standards and network effects trap governments within commercial ecosystems even when the costs – financial or strategic – become hard to justify. The third is the question of democratic control of systems that are not politically neutral. Decisions about how infrastructure operates, what it prioritises and how it

TECH GIANTS AND GIANT SLAYERS

evolves have political and social consequences, whether or not they are made through political processes.

The fourth danger is perhaps the deepest. Data and algorithms do not merely power economic activity. They increasingly mediate how citizens encounter information, interpret events and form political opinions. The systems that curate what we read and watch now have the power to shape public debate itself. We have already seen how foreign-owned platforms can promote, suppress or algorithmically amplify particular viewpoints – sometimes reflecting the preferences of their owners. Control over digital infrastructure therefore extends beyond markets and innovation into something more fundamental: who shapes the public sphere, and on whose terms.

This is the digital equivalent of what some of us are calling ‘the privatisation premium’. When essential services are privatised, households and businesses typically end up paying more for infrastructure that once existed to serve the public interest. Water, energy, rail and housing have all shown how private ownership of natural monopolies produces higher costs, reduced accountability and systemic extraction. In the digital realm the same dynamic is at work – but the cost is not simply financial. Those who control data and the systems built on it can extract value from it, train the algorithms that define future markets and capture the economic returns that follow. Control of infrastructure today means control of innovation tomorrow.

The report points towards solutions, among them the revival of a principle Britain once understood well: that certain forms of infrastructure are too important to be left entirely to market forces.

The creation of the BBC offers a useful precedent. When broadcasting emerged in the early twentieth century, Britain faced a choice between the American model – private corporations dominant, commercial incentives paramount – and a public institution designed to serve the public interest. Under John Reith, Britain chose the latter. Reith warned in 1924 against allowing private corporations to dominate communications networks, and insisted that broadcasting should operate within a framework of democratic accountability. The institution that resulted has lasted a century.

As the BBC approaches its next Charter renewal, that choice presents itself again in a new form. This is not merely a debate about broadcasting. It is a moment to

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

consider the broader role public institutions can play in the digital public sphere – whether a renewed BBC, embedded within a wider ecosystem of open technologies and publicly accountable infrastructure, could help anchor a genuinely public digital commons.

The challenge is not technical. It is political. It concerns the shape of power in the twenty-first century, and whether democratic institutions retain the capacity to exercise it. The East India Company director who described his enterprise as a sponge was at least honest about what he was doing. The question before us is whether, two hundred years later, we are equally clear-eyed about what is happening – and whether we retain the will to respond.

EXECUTIVE SUMMARY

RECLAIMING DIGITAL SOVEREIGNTY

- **Digital Sovereignty is critical for the UK's economic and national security.** It is defined as the ability of a country to have control over its digital infrastructure, data, and technology.
- **The UK is currently facing a crisis of digital dependency.** The country is overly reliant on a small number of tech giants for its critical digital infrastructure, which poses significant economic, security, legal, and policy risks, including to democracy and public debate.
- **A strategic shift to using and growing the Digital Commons – that is, open technologies – provides the most effective path to Digital Sovereignty.** This includes shared Open Source software, open standards, and open hardware, which can foster a more competitive and innovative domestic tech sector, reduce costs, and enhance security.

THE HIGH COST OF DIGITAL DEPENDENCY

In *Part I The Digital Sovereignty challenge* we find:

- **Economic risks:** The dominance of a few tech giants leads to vendor lock-in, inflated costs for government and businesses, and the extraction of value from the UK economy through tax avoidance and profit repatriation.
- **Security risks:** Reliance on foreign proprietary technology creates vulnerabilities to surveillance, espionage, and cyber attacks. These risks are produced by foreign legal frameworks, which govern both US and Chinese technology companies.
- **Surveillance risks:** The UK is exposed to the extra-territorial jurisdiction of other countries, such as the US Clarifying Lawful Overseas Use of Data (CLOUD) Act and China's National Intelligence laws, which can compel tech companies to hand over data.
- **Policy Risks:** The immense lobbying power of Big Tech distorts policy-making, leading to weaker regulation, anti-competitive practices, and a centralised, abusive and anti-democratic digital information environment.

THE UK'S CURRENT POSITION:

Part II Current UK policy position shows that:

- **The UK lacks a coherent Digital Sovereignty strategy.** Current policies are designed to reinforce dependency on foreign tech giants.
- **The Government's analysis of the 'chronic' risks is classified,** precluding public debate of its approach.
- **Government IT procurement is dysfunctional.** It is characterised by a lack of competition, vendor lock-in, and a series of high-profile project failures and cost overruns. Like other areas of government procurement, there is not a functioning market, so government cannot expect good procurement while it is a passive recipient of software services. There is insufficient focus on known solutions to resolving this dysfunction. Solutions include: leadership in development and ownership of custom software; requirements for interoperability; preferencing Open Source; and leveraging competition policy in the cloud market.
- **Competition and data protection enforcement have been weakened.** This invites tech giants to further consolidate their market power and continue to engage in anti-competitive practices. It appears to be a response to dependence, seeking to attract further inward investment that will build economic extraction rather than reduce it.

DIGITAL SOVEREIGNTY REDUCES COSTS AND GROWS THE DIGITAL ECONOMY

We show in *Part III Beyond the UK* how other countries are benefiting from prioritising Digital Sovereignty.

- **Building the economy:** Germany, France, Netherlands, Denmark and other European nations are actively pursuing Digital Sovereignty through strategic investments in open technologies and international collaboration.
- **International collaboration:** provides a model for governments to create and control key technologies for common problems, including in health, data and procurement.

THE OPPORTUNITY OF THE DIGITAL COMMONS

- Growing the Digital Commons with Open Source software offers a major opportunity for the UK in modernising critical government systems and strengthening control over public technology infrastructure.
- It can repair the relationship between government and the technology it relies on, by reducing dependence on proprietary vendors and restoring public sector control.
- Greater investment in Open Source can also **drive UK economic growth**, supporting domestic innovation and a more competitive technology sector.
- Despite underpinning much of the global digital economy, Open Source remains **underrecognised in UK government strategy**.
- National economies would be **2–3% smaller without Open Source software**.¹
- Open Source is present in **over 95% of proprietary software systems**, making up **around 70% of their codebase on average**.²
- EU research suggests **every £1 invested in Open Source returns around £4 in economic value**.³
- The Linux Foundation estimates **2–5x return on investment for organisations contributing to Open Source**, rising to **around 6x for leading contributors**.⁴
- France's **government preference for Open Source procurement**⁵ helped generate **9–18% annual growth in IT startups**, while also creating globally valuable Open Source assets.⁶
- In the UK, OpenUK estimates Open Source contributes **around £13 billion annually**, representing **27% of the technology sector**.⁷
- A 2024 Harvard study estimates the **global demand-side value of Open Source at \$8.8 trillion**, noting firms would need to spend **3.5x more on software without it**.⁸
- European Commission research suggests **a 10% increase in Open Source contributions could add 0.4–0.6% to annual European economic growth**.⁹

THE WAY FORWARD: A ROADMAP TO DIGITAL SOVEREIGNTY

See *Part IV Recommendations for a Digital Sovereignty strategy*.

- **Embrace the Digital Commons of Open Source:** The UK should adopt a "Public Code for Public Money" policy, where software developed for the public sector is made available under an open source license.
- **Strengthen competition and regulation:** The UK must empower its regulators to challenge the market dominance of tech giants and enforce pro-competitive measures, such as interoperability and data portability.
- **Build digital leadership in Government:** The UK needs to rebuild its in-house technical expertise to reduce its reliance on external consultants and make smarter procurement decisions.
- **Foster international collaboration:** The UK should actively participate in international initiatives to develop open standards and digital public goods, and collaborate with other countries on strategic technologies like AI and cloud computing.

KEY RECOMMENDATIONS FOR THE UK GOVERNMENT

For the full recommendations, see *A Roadmap for Digital Sovereignty*.

- **Reset UK digital policy** to make Digital Sovereignty a central strategic goal.
- **Drive competition and effective regulation** to create a more level playing field for UK businesses.
- **Deliver 'Public Code for Public Money'** to build a commons of publicly-owned software.
- **Invest in the UK's Open Source ecosystem** through procurement, tax incentives and skills development.
- **Build digital leadership** within government to drive the transition to open technologies.
- **Protect democracy** by promoting a more diverse and open social media landscape.

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

INTRODUCTION

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Is the UK in control of its critical tech, national infrastructure and digital policy making? That is the question that the Digital Sovereignty debate raises. While the risks from one-sided digital dependency are significant, the benefits of promoting autonomy combined with international collaboration are compelling.

Risks of dependency have recently been thrown into sharp relief. They were first recognised by the UK in relation to Chinese network infrastructure. Huawei, which has supplied equipment for use in 5G networks, came under scrutiny for the potential for 'backdoors' in network software to be used for surveillance, shutdowns or to aid attacks.

The question was raised again by the USA's decision to sanction the International Criminal Court (ICC), leading to Microsoft shutting down its email facilities, and the closure of electronic and online banking facilities to ICC members.¹⁰ Denmark has been forced to consider the potential that it will face retaliatory action in the event of disputes over the future of Greenland.¹¹

Disputes over Greenland or other foreign policy interventions threaten to create friction between the UK and the US. In the event of a falling out, tech dependency could easily become instrumentalised, whether through surveillance, price hikes, service withdrawals or suspensions, or the threat of any of these. Far from being wild suggestions, UK commentators including staff at the Royal United Services Institute (RUSI) are asking deep questions about these risks.¹² UK banks are taking action to protect themselves from the US card payment systems.¹³

Dependency on large tech providers has negative consequences for human rights and democracy. Big tech companies such as Palantir have been accused of promoting intrusive policing and surveillance.¹⁴ Big tech intervenes in policies regarding online safety and free expression, and – for example in the case of Musk and X – stands accused of seeking to shape online democratic debate according to its owners political preferences.¹⁵ Tech leaders are able to promote politics that are in their own interests and that may run counter to basic democratic norms.¹⁶ Ideologies that are evolving and promoted by big tech appear designed to help their profits grow ever higher, at the cost of democracy and rights.¹⁷ We discuss these dynamics below at *Online political distortion*.

The risks outlined so far are just the sharpest end of the UK's dependence on transnational companies' technologies, especially their proprietary tech. As we discuss below, at *Economic dependency and extraction* and *Impact of UK tech*

TECH GIANTS AND GIANT SLAYERS

companies being sold to tech giants, dependence takes a heavy economic toll, as profits, expertise, and employment shift, particularly to the US. Furthermore, dependence is skewed towards a small number of dysfunctional relationships with IT system suppliers and consultants. Where these are headquartered outside of the UK, there are risks that they will seek to minimise their financial liabilities through offshoring profits.

While the challenges are significant, the benefits the UK can accrue from change are enormous. If dependence means extraction, then independence can mean economic growth, jobs and successful IT systems. What is more, a growing number of governments are already making exactly these kinds of changes.

As shown in *Defining Digital Sovereignty* in Part I of this report, many governments have identified that the Digital Commons, especially Open Source and open standards, is key to securing future Digital Sovereignty. This approach gives governments autonomy and control of operation, development, deployment and data, especially where IT systems are brought back in house. These tools have long been identified in UK policy as key to ensuring government can control their relationships with IT vendors and improve reliability, as discussed in *Vendor lock-in*. All relationships with proprietary software suppliers tend to suffer problems with 'satisficing'¹⁸ contracts, that is, providing minimal compliance and taking the reward while leaving government with the risks that come with major IT projects. As we explore in *UK spending on digital technologies*, and summarise in *Appendix IV UK tech strategic suppliers*, currently around eight major IT providers and consultancies named as strategic suppliers to the UK are overcharging, while others are causing projects to overrun budgets and ensuring long-term dependence on their systems, whether good or bad.¹⁹ To that list, which includes Accenture, Oracle, and Microsoft, we can now add Palantir. Vendors are chosen because of existing dependency or convenience, or sometimes because it suits the Treasury to shift software investment costs off government books. The results have been disastrous.²⁰

However, the benefits of Open Source go much further. National economies would be around 2-3% smaller if Open Source did not exist,²¹ and Open Source software is found in over 95% of proprietary systems, making up over 70% of such products on average.²² It brings back an average £4 for every £1 invested.²³ Without Open Source, firms would be spending 3.5 times more on software.²⁴ French leadership in Open Source and open weight AI have contributed to a 9-18% growth in tech

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

start ups.²⁵ When Open Source is used, local IT vendors, including Small and Medium-sized Enterprises (SMEs) can often more easily compete for contracts, and through specialisation can even have the advantage over the tech giants.

With such significant economic returns, it is startling that Open Source does not seem to be a strategic priority for the UK, even without sovereignty concerns. As we set out in *Part III Beyond the UK* a growing number of governments are finding ways to leverage the Digital Commons of Open Source through collaborating on major IT systems that are re-used in multiple countries.

The result is autonomy and interdependence, technology transfer to the developing world, and competitive IT markets. International trade and software markets become safer. Collaboration between governments to share software code creates efficiencies for everyone. The UK can lead tech where it wants to, and use tech to develop our own soft power. As we show in *Part III Beyond the UK* Germany, France, Scandinavia, Baltic countries, Switzerland and India are already making these kinds of gains in the fields of health, data infrastructure, AI and productivity software, among others.

This is not to say that it is always easy to choose Open Source or that Open Source is always a plausible choice today. Rather, over time choosing Open Source can be optimal for sovereignty, value for money and economic growth. And often, reaching the objective of Digital Sovereignty requires the Digital Commons of Open Source in practice. To make this happen, as we set out in *Part IV Recommendations for a Digital Sovereignty strategy*, there needs to be a strategic shift in the way we approach vendors from dependency and accepting dysfunctional markets to achieving autonomy over government systems and promoting economic development through our approach to software procurement and our wider tech strategy. The UK needs to develop capacity to manage and develop Open Source systems and markets, as other governments are doing. The UK has led this change before, under both Labour and Conservative governments. It needs to return to what it has already learnt and push again, harder, to meet geopolitical risks and our economic goals.

PART I

THE DIGITAL SOVEREIGNTY CHALLENGE

DEFINING DIGITAL SOVEREIGNTY

Discussions are taking place in many countries over Digital Sovereignty, or the extent to which a country is in control of its critical tech infrastructure. One definition is:

the right and ability of political entities to autonomously (independently and/or self-determinedly) use and control tangible and intangible assets and digital services that significantly impact democracy, the economy and society²⁶

Digital Sovereignty has been a theme of French policy since 2017.²⁷ The French government's digital strategy has four objectives, of which one is to "preserve the Digital Sovereignty of the state by investing in shared digital tools", in other words, identifying Open Source as the method.²⁸

The former German Chancellor, Angela Merkel, turned to the topic in 2019.²⁹ Since then, the 2022 German government set an objective of "strengthening our Digital Sovereignty, for instance by promoting innovation in a targeted manner, improving expertise in key technologies and promoting open source"; it also referenced the Digital Sovereignty of the individual.³⁰ Under Merz, sovereignty has shifted to meaning "the ability to shape technology across the entire value chain in line with European interests and needs".³¹

Different visions centre on technical, data or Internet sovereignty, as well as personal self-determination. Discussions have grown at pace since 2011, in part fuelled by the 2013 Snowden revelations, which highlighted the vulnerability of systems and countries to US-UK surveillance,³² and by the emergence of cloud technologies.³³ There are, as Stephane Couture and Sophie Topin note, risks in summoning up the idea of sovereignty, rooted in the nation state, potentially obscuring the interdependence of a globalised world and ignoring the differences between different countries to avoid unequal and unfair relations.³⁴ However, if states engage in international open collaboration as outlined in *Part III Beyond the UK*, there is also a vision available of mutual gain, national autonomy, and trust. Hermann Hauser believes that interoperable and open technologies are the natural route for collaboration and interdependence between blocks of states, particularly the US, China and Europe, positioning this as a choice that avoids

TECH GIANTS AND GIANT SLAYERS

dependency and economic coercion risks.³⁵ Konstantin Komaitis emphasises the idea of “interoperable sovereignty”, meaning technical, regulatory, and institutional interoperability – in other words, creating strengthened sovereignty through collaboration to build shared norms and standards.³⁶ Some discussions have highlighted the choices that Digital Sovereignty gives for different environmental and social outcomes.³⁷

The term ‘Digital Sovereignty’ is understandably contested, as some visions of it verge on autarky, or promote state control and surveillance.³⁸ ORG rejects these, and uses the term pragmatically as the established concept in Europe, rather than out of any nationalism.

The Tony Blair Institute (TBI) has rejected what it sees as a “narrow and ultimately counterproductive understanding of sovereignty, particularly regarding AI policy: one that equates autonomy with full technological control and treats interdependence as a vulnerability to be eliminated”. Instead, it says: “Sovereignty ... is fundamentally a question of agency and choice – the ability of a state to make deliberate, future-oriented decisions about how AI is integrated, governed and used in line with its national goals” to ensure “strategic autonomy and expand national agency over time.”³⁹

The TBI's portrayal of the positions in the debate sets up something of a straw man; the real question is more what counts as actual risk, effective decisions, national goals and agency. TBI leans towards interdependence and leveraging AI benefits as a strategy for managing sovereignty. By contrast, the debate in the US has not been defined as Digital Sovereignty, but rather as maintaining control of the tech market globally, and winning or losing in competition with China.⁴⁰ They do not appear to be aiming for interdependence. TBI's approach risks delivering one-way digital dependence while casting it as 'sovereignty'.

Discussions at national and international level are focusing on (a) risks in the event of foreign policy and trade conflicts; (b) risks for supply chains if key technologies are unavailable; and (c) the need for countries to build a thriving tech sector and expertise as a strategic economic asset. The impact of cloud and AI have had significant impact on the framing of the debates, because of the acute importance and difficulties of avoiding dependence. Meanwhile, chip and supply chain problems following Covid awoke European industries to the risks of over-reliance on Asian manufacturers.

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

The EU's definitions for 'sovereign cloud' contracts reflect these broad risks and include criteria for categories of sovereignty approaches: strategic, legal, data and AI, operational, supply chain, technology, security and environmental.⁴¹

The political dimension of tech dependency also be seen as a core problem of Digital Sovereignty. This includes risks of Big tech lobbying for lower taxes and business benefits, disadvantageous trade agreements, and distorting the information ecology in favour of tech oligarchs' personal agendas.

CREATING TECH DEPENDENCY

COMPETITION IS FOR LOSERS

Digital tech dependency has been recognised as a problem for a long time. Costs of switching vendors were observed to be the "the norm, not the exception, in the information economy" in 2002.⁴² The problem extends across business and society as well as government; in 2025, Boston Consultancy Group found that vendor lock-in concerned 62% of IT buyers who were using cloud software platforms.⁴³ Vendors find many different ways to create customer dependency, as from the seller's perspective it is a means to ensure business continuity and maximise profits. This approach was recently summed up by Peter Thiel, founder of PayPal and Palantir, in his essay *Competition is for losers*, citing the difference between competitive airline pricing and Google's monopoly on search:

...capitalism and competition are opposites. Capitalism is premised on the accumulation of capital, but under perfect competition, all profits get competed away. The lesson for entrepreneurs is clear: If you want to create and capture lasting value, don't build an undifferentiated commodity business ... Monopolies drive progress because the promise of years or even decades of monopoly profits provides a powerful incentive to innovate. Then monopolies can keep innovating because profits enable them to make the long-term plans and finance the ambitious research projects that firms locked in competition can't dream of.⁴⁴

In other words, once profits are secured through vendor lock-in, further investment leads to further products that produce future lock-in. While this model may be attractive to the handful of global winners in the tech market, it is not so

TECH GIANTS AND GIANT SLAYERS

appealing the for businesses, citizens and governments on the receiving end of this approach, who, according to Thiel, will experience higher prices, dependency and a lack of practical choice.

Analysts question whether companies are genuinely providing value or are in fact merely seeking means of establishing rents. Many online markets are multi-sided: the platform mediates the relationships between customers seeking services and the suppliers of those services.⁴⁵ By acting as the gatekeeper between customer and supplier, a company can shape the market and extract payments.⁴⁶ For example, Amazon is the easiest way to purchase many goods online; Uber sought to become the way that everyone finds a taxi; AirBnB is the default way for people to find cheap temporary accommodation.

This business strategy depends on leveraging investment capital so that the business can run losses while attracting a potentially massive user base in the hope of achieving a future monopoly. Once users and suppliers are dependent on the marketplace, the platforms may raise fees and exploit service terms and conditions to create a return on the investment. While Thiel claims this arrangement is somehow liberating, it can be shown that it causes user experience to deteriorate, and allows monopolies to leverage profits from companies dependent on them through price fixing, a process called 'enshittification'.⁴⁷ This is neither good for the economy as a whole nor for innovation, if we believe that competition is the normal route for new technologies to find new consumers.

VENDOR LOCK-IN AT GOVERNMENT

Vendor lock-in within government systems can be created in myriad ways. In brief, strategies include:

1. Proprietary software and secret code: a program is sold under the condition that only the end user may use it, and they are given the software without the ability to modify it. Changes and updates come from the vendor alone.
2. Restrictive licensing: customers can be forced to use particular systems, as with Microsoft's cloud products, which require additional fees if a customer wishes to use a different cloud provider.
3. Punitive exit (egress) fees: with cloud products, customers are charged for exporting their data when they leave the service.

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

4. Skills and knowledge: when a technology is dominant, it becomes costly to retrain users in a new system.
5. Technical lock-in: proprietary interfaces and data and file formats increase the difficulty of exiting from a vendor's technology.
6. Ecosystem effects: plug-ins, macros, and third party software added to the original product raise the costs of exit. For example, an Apple iPhone user may have paid for apps which they will need to repurchase if they move to an Android phone. Providing free accounts to students or civil society can similarly hook users into specific software systems.
7. Bundling of services: for example, providing office technologies with operating system and cloud services, makes it difficult to impossible for purchasers to opt out of any part of the cluster of technologies, as the journalist Kashmir Hill showed at the individual level in 2019.⁴⁸

The more fundamental the technology the better, from the vendor's point of view. Replacing the back end infrastructure, the operating system or the custom government system is likely to be expensive and inconvenient. Cloud systems apply extra charges for removing client data and encourage clients to use proprietary management tools that cannot be replaced without significant effort. There are similar concerns with new AI technologies, which are increasingly embedded into and build on existing locked-in software systems.

Governments have a series of tools they can use to avoid vendor lock-in, such as insisting on interoperable software, and adhering to commonly used open standards. However, major vendors are resistant to both of these basic requirements, precisely because they undermine their monopoly position.

The UK's experience is discussed at *UK spending on digital technologies* and *Appendix IV UK tech strategic suppliers*.

CONSULTANCY AND AUDITORS

Consultancy is another factor in vendor lock-in. While external consultants should be vendor neutral, in practice they tend to have strong relationships with, and knowledge of, specific vendors.⁴⁹ They often have long contracts to build and run government IT systems. Even when producing Open Source code, they typically use internal code management systems, which make it difficult to share the code between agencies.⁵⁰ By building up familiarity with departmental

TECH GIANTS AND GIANT SLAYERS

systems and the solutions that are implemented, they become deeply embedded in Whitehall departments, to the point where it becomes prohibitively difficult to remove them. Their knowledge and commitment to existing systems creates a brake on further change and helps cement existing vendors into their relations with government, even when the results are poor. Conflicts of interest are endemic in the consultancy-government relationship, and their advice is likely to be aimed at gaining further business and contracts rather than improving government capacity to manage.⁵¹

All of the big four audit firms that regularly assess public sector value-for-money have established partnerships with large technology companies, including Microsoft. These companies offer advice about efficiency gains they can make with their partnered vendors. For example, PwC is a designated Microsoft Solutions Partner and was recognised as Microsoft's 2024 Partner of the Year for AI and Government, reflecting PwC's role in implementing Microsoft technologies. PwC's Global Microsoft Alliance Leader, Stephanie Mosticchio, explained that:

Copilot is not just a tool – but a platform for end-to-end transformation and to enable clients to get impactful products and offerings to market quicker and at a fraction of the cost. This is why we are excited to collaborate with Microsoft, to share the power of agentic AI with our broad client base.⁵²

Likewise, KPMG maintains a strategic alliance with Microsoft, currently focused on AI.⁵³ Deloitte also offers Microsoft Technology Services⁵⁴ and Grant Thornton is a Gold Microsoft Partner, also promoting its AI products.⁵⁵ The potential for conflicts of interest in this very concentrated market was examined in 2024 by the Australian Parliament, who questioned the partnership model.⁵⁶ Moving in the opposite direction, the US Securities and Exchange Commission (SEC) are looking at allowing looser relationships, noting that “because large accounting firms now sell software and AI tools from companies such as Microsoft and OpenAI, they are often barred from auditing those same firms”. The SEC says this may unfairly limit the choice of auditors for large tech companies,⁵⁷ but removing this bar would only further cement the close and conflicted relationship between major tech vendors and accountancy-consulting firms.

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

CLOUD AND AI LOCK-IN

Cloud lock-in is maintained in similar ways, for example by offering technical features and proprietary programming interfaces which developers cannot easily dispense with once they have decided to rely on them.⁵⁸ Cloud lock-in is exacerbated by the limitation of the market to three operators, Amazon Web Services, Microsoft, and Google; they offer global demand management, scale and pricing that others cannot currently match.⁵⁹ Fees for removing data from systems ('egress fees') help cement lock-in.⁶⁰ Microsoft leverages its market position by charging more for its software if the customer does not use Microsoft's cloud service, Azure;⁶¹ this costs the UK £500m in excess fees, according to the CMA,⁶² and around €1bn in Europe in 2023.⁶³

The move to cloud has technical benefits, such as ease of management and demand management, but this has made reliance on proprietary products even more of a competition and lock-in risk. The capture of the basic technical resources and the cash piles resulting from claiming rents for access to computing capacity have placed the cloud giants in a position to launch ever more cloud and AI capacity and dominate the current AI landscape, with the ambition to profit further in future despite currently low revenues.⁶⁴

However, AI technologies such as LLMs do not necessarily require supercomputing facilities.⁶⁵

LOBBYING AND ASTROTURFING

Maintaining vendor lock-in is no small feat, as it results in higher costs and poor value for money for governments. Microsoft have frequently stamped out efforts by state authorities to move away from their systems.⁶⁶

Oracle is promoted aggressively to Global South and middle eastern governments by the TBI, according to recent investigations.⁶⁷ At least one member of staff from TBI has been seconded to the UK government's Department for Science, Innovation and Technology (DSIT) to work on the UK's Sovereign AI project while still on the TBI's payroll.⁶⁸ Palantir and Foundry appear to have got a foothold in the UK through close personal links with Boris Johnson's special advisor Dominic Cummings,⁶⁹ and through Peter Thiel's connections to disgraced former US ambassador Peter Mandelson and sex trafficker Jeffrey Epstein.⁷⁰

TECH GIANTS AND GIANT SLAYERS

While Parliament has been focused on the worst outcomes from social media giants, it has also given the Competition and Markets Authority (CMA) new powers to tackle their monopoly power, along with Amazon and other cloud providers.⁷¹ Silicon Valley's response was to lobby against these powers being used. Ministers and advisors including Chancellor Rachel Reeves, Secretary of State for Business and Trade Peter Kyle,⁷² and Varun Chandra,⁷³ a special advisor to Keir Starmer have been accused of being close to the tech industry, which has clocked up 639 meetings with ministers. Google alone has had over 100.⁷⁴ The 2024 Labour government has appointed a former Amazon executive to head the authority⁷⁵ claiming that a new appointment was needed to deliver the government's growth agenda,⁷⁶ with analysts suggesting it was done to build confidence with the tech industry in advance of future AI and cloud investments.⁷⁷ Simultaneously, they also instructed the CMA to ensure it did not act too strongly.⁷⁸

Lobbying also extends to astroturfing. Currently, a number of AI investors have been found to be paying for AI safety campaigns, which either aim for industry self-regulation or raise the alarm on apparent existential threats of AI. The latter appears to be an effort to avoid regulation of the actual problems, such as bias and discrimination.⁷⁹

TRADE AGREEMENTS

Closely related to lobbying is the use of trade agreements to promote vendor interests. Trade negotiations always include close involvement of trade associations and major industrial players.⁸⁰ Treaties are increasingly bilateral rather than led at the UN level, causing persistent democratic risk, as they are negotiated in secret. In the UK, this is made worse by the fact that the UK Parliament is neither involved in nor afforded access to the negotiation process, nor has the right to vote to ratify or decline the treaty, in contrast to the US and EU legislatures.⁸¹

The US is experienced in ensuring that its own economic needs, such as strong intellectual property⁸² and data flows across borders are prioritised in trade agreements over questions such as the right to repair devices (which can be restricted through patents and copyright)⁸³ and data protection (which can hinder data moving to less regulated spaces). This can even extend beyond the US's official policy position to the preferred stance of trade lobby groups.⁸⁴ Online safety

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

has become a new area of contention, as regulatory demands from UK and Europe are seen as attempts to restrict tech companies from promoting political positions favourable to Trump. The US has even placed visa bans on EU officials.⁸⁵

While the UK has resisted trade treaty clauses that would pose problems related to online safety, there are other concerns with agreements we have struck regarding data flows. In particular, the model of data protection enshrined in the Trans-Pacific Partnership (TPP) allows for private, non state voluntary regulatory agencies to act to ensure data is protected. Such bodies cannot, for example, resist requests from government surveillance agencies, nor guarantee the rights of individuals in such circumstances. However, the TPP facilitates such data flows. The TPP also commits the UK to not prioritising data protection of data flows beyond the minimum necessary for policy goals. Current data protection may rightly be more protective than the “minimum” in every circumstance.⁸⁶

Trade policy also includes discussions on investments and companies' entry into the UK. The model of US investment in the tech sector, such as building data centres to supply access to US-built AI technology, will certainly benefit US companies but will not provide high levels of quality employment for the UK.⁸⁷

REMOVING THE RIGHT TO REPAIR AND PREVENTING AI TRANSPARENCY

Trade policy may deliberately attempt to preclude the repairability of devices, by demanding that Technical Protection Measures (TPMs) must be legally protected by the contracting governments.⁸⁸ TPMs are meant to protect copyrighted works, for example copy protection in DVDs and Blu-Ray disks. It is unlawful to discover how to break the copy protection or to help others to do so. However, many electronic devices contain TPMs which are designed to stop embedded software from being interfered with. The software and hardware may be protected by copyright, design rights and patents.⁸⁹ Trade agreements promoted by the US in particular have aimed at preventing the users from replacing embedded software by demanding legal protection against circumventing TPMs.⁹⁰ Provisions demanding that access to source code must be prevented can also be used in the same way.

However, users are often forced to bypass TPMs to keep mobile devices, e-readers, and the like functioning. When manufacturers stop updating software or remove remote support, the device can become either insecure or 'bricked'. The result is trade treaties likely to generate e-waste.⁹¹

TECH GIANTS AND GIANT SLAYERS

Clauses limiting access to source code can also be aimed at limiting preventing government software transparency, critical for security auditing, and barring transparency requirements for algorithms and AI systems.⁹²

CHIPS AND DEVICES

In recent years, chip shortages have hit European manufacturers, highlighting the fact of dependency on a very small number of chip manufacturers and vendors. The problem is more acute because electronic devices of all kinds often include embedded software and remote management.

Chip manufacturing is expensive and very concentrated. High-end chips are produced by one Taiwanese company, TSMC, although the company is now building factories in the US following Biden's Chips Act.⁹³ The Dutch company ASML produces 83% of the tools to etch chips,⁹⁴ and only three companies control the chip design market, including ARM, a UK-founded company which is Japanese-owned and US-listed. Moving software from one chip architecture to another is costly, helping to keep Intel in its lead position despite lagging in the efficiency of its processors. Operating system vendors choose which chip designs they will support, thereby locking their users into particular vendors.

Chip designs are tightly controlled through intellectual property rights, causing prices to be artificially high and reducing the ability of device manufacturers to innovate through chip customisation.

Proprietary control affords chip designers opportunities to attempt to control the whole computer, for instance to dictate what may be installed. This may be presented as a 'security' feature, as in the case of Secure Boot, which makes it hard to install Linux on Windows machines.⁹⁵ Similarly, chips can be engineered to provide backdoors to the whole system, either deliberately or accidentally. This has been noted in designs from both Chinese companies and Intel, whose "Intel Management Engine", was found in 2015 to create risks of remote access.⁹⁶

Devices are frequently locked to specific software systems. For example, the footage from CCTV cameras may be recorded by a data centre, or a vehicle may receive software updates from its manufacturer. These lock the user and device to the software vendor. As noted above, this is often exacerbated by the device manufacturer taking measures to prevent its software being removed and replaced with generic software, causing working devices to cease functioning when the manufacturer ends support.

RISKS FROM BUSINESS AS USUAL

LEGAL RISKS

As most services are based in the US and technologies are often manufactured in China, the duties they impose on software and hardware vendors are most important to assess. Both countries create duties which could be used to access or exfiltrate data for surveillance purposes. The US also can employ the power to sanction – that is, to direct tech companies to sever commercial relations.

US POWERS OF ACCESS

US companies are subject to the Foreign Intelligence and Security Act (FISA), which grants US security services direct access to data stored by US-owned companies. While the nature of these powers was denied, their usage was confirmed in 2013 by the Snowden revelations. A request for access to cloud storage in Ireland was granted to the US government by the US courts in 2018 in *Microsoft Corp. v. United States*.⁹⁷ Soon afterwards, the CLOUD Act of 2018 attempted to further clarify the legal basis for lawful access and to give other countries similar rights of access on the basis of mutual agreements.⁹⁸ The case also led to Microsoft's frank admission that it could not “guarantee” the data sovereignty of European governments' data stored in its cloud.⁹⁹

In the EU, the powers to access data stored within the US was challenged on the grounds of a lack of accountability and lack of access to individual redress. These cases, known as Schrems I and II, brought down two US-EU data protection agreements, “Safe Harbor” in 2015 and “Privacy Shield” in 2020.

US POWERS OF SANCTION

The US also has powers of sanction, which can be used to stop a company from supplying a government, institution or individual with services. The International Emergency Economic Powers Act (IEEPA) of 1977 grants sweeping powers to the US president to issue an Executive Order declaring a national emergency.¹⁰⁰ Although the Act originally granted Congress the right to veto, this provision was found to be unconstitutional in 1983.¹⁰¹ As a result, the President can simply declare a national emergency and exercise IEEPA's powers, including stopping individuals and corporations from conducting business with people on the sanction list. This allows the US government to order companies including VISA

TECH GIANTS AND GIANT SLAYERS

and Mastercard, to cease doing business with an individual, cutting them out of most online transactions, effectively conferring a “financial death sentence”.¹⁰² Companies like Google and Microsoft can be ordered to cease supplying an individual or “entity”, although speech protections in the Act theoretically should stop bars on using services like email. The Office of Foreign Assets Control (OFAC) administers sanctions against foreign regimes and persons.¹⁰³

Although originally intended to be used sparingly, IEEPA powers were exercised 11 times in Trump’s first presidency¹⁰⁴ against 2,800 individuals.¹⁰⁵ The widely criticised sanctions US President Donald Trump imposed in his second presidency against members of the International Criminal Court (ICC) for investigating Israel’s Prime Minister, Benjamin Netanyahu for genocide in Gaza¹⁰⁶ are a repeat of his behaviour in his first presidency, when he sanctioned ICC officials for investigating the US for war crimes in Afghanistan.¹⁰⁷

CHINESE POWERS TO DIRECT TECH COMPANIES

China’s powers are extensive and opaque. Chinese security services are well resourced and powerful. National security legislation gives China extensive powers to oblige private sector cooperation, while the state also runs a ‘Military-Civil fusion’ strategy, aimed at insuring that the People’s Liberation Army can access private sector technologies both domestically and abroad. While this ‘fusion’ appears to be aspirational, and in some ways is modelled on the US’s technology transfer between civilian and military sectors, the legal potential for coercion is clear.¹⁰⁸ There are legal obligations that apply to everyone and all organisations in China to provide evidence and assist state security organs.¹⁰⁹ Network operators must give technical support to public and security services for criminal and national security investigations,¹¹⁰ and data localisation is compulsory in order to ensure lawful access by the authorities.¹¹¹ Access to and decryption of data for terrorism purposes is compulsory, effectively compelling backdoors in encrypted technology.¹¹² While legal powers may not be routinely exercised, and companies may introduce friction around compliance,¹¹³ from an external perspective such powers are extremely worrying.

There is evidence that these powers may have been used in relation to Huawei’s equipment, which was due to be supplied to the UK for the 5G rollout.¹¹⁴ A security audit by Finite State found the company’s devices to be riddled with security vulnerabilities, including stored access credentials. However, it is a matter of judgement whether the Huawei’s embedded software was simply badly designed

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

and maintained or contained deliberate means of access, or both.¹¹⁵ A 2018 *Bloomberg* investigation claimed to have found vulnerabilities in chips manufactured during the 2010s for the US firm Super Micro Computer Inc, a supplier to Apple and Amazon, and that evidence of tampering at Chinese manufacturing facilities had been covered up by US authorities. *Bloomberg* went on to claim that Super Micro servers were routinely reporting device and network information back to China and that the problem was detected and used to investigate Chinese intelligence agencies' practices.¹¹⁶ Concerns over the Chinese laptop manufacturer Lenovo have continued for many years. In 2014, Lenovo began including the Superfish spyware with some of its machines,¹¹⁷ and intelligence agencies put bans in place during the 2010s. The company remains a UK supplier, including for the UK's national supercomputer project.¹¹⁸¹¹⁹

Worries around the potential for attacks have led the US to exclude Chinese tech from some sectors, including electric cars. The *Financial Times* has reported that Chinese electric vehicles have also been banned on UK military bases.¹²⁰ US policy now has a wide range of measures designed to exclude Chinese products from various market sectors due to risks of Chinese intervention. However, a recent Carnegie Endowment for International Peace report warns that this policy is not coherent and could present risks if Chinese competition is shut out.¹²¹

ECONOMIC DEPENDENCY AND EXTRACTION

The security risks already identified easily flow into imposing price hikes and poor value for money on governments. The economic risks to the UK are in fact much wider, given how much money the government spends on hardware and software. When software systems are foreign owned, maintained and controlled, the skills, work, and profits are exported. This relocates value outside of the UK, depressing the size of the tech sector and reducing the UK corporate tax base. Similar trends can be observed across the UK economy, but the effects are particularly intense in the tech sector.¹²²

The risks of the current economic strategy of foreign acquisitions and inward investment have been highlighted by RUSI who question the impact on sovereignty if UK tech is "funded, designed, built, and operated by American companies".¹²³

TECH GIANTS AND GIANT SLAYERS

IMPACT OF UK TECH COMPANIES BEING SOLD TO TECH GIANTS

If sovereignty risks can be mitigated through interdependence, then development of key technologies within the UK helps manage risk overall. In recent years, several leading technology firms have been sold to US providers, creating the risk that expertise and value from these firms flows overseas while reinforcing dependence on US tech. Foreign sales of UK tech companies appears to have accelerated since the 2024 election, accounting for 55% of acquisitions in 2025.¹²⁴

The most controversial of these sales included the sale of DeepMind to Google,¹²⁵ and ARM to Japanese investor Softbank.¹²⁶ Softbank later attempted to resell ARM to NVIDIA, but was blocked by the US Federal Trade Commission on competition grounds.¹²⁷ ARM's profits, like those of DeepMind, now mostly accrue overseas. A list of other controversial tech acquisitions can be read at *Appendix I UK tech companies sold overseas*.

The largest foreign acquisitions have concentrated on the most strategic UK companies, targeting multiple companies in strategic areas including chip manufacturing and machine learning and big data, or what is now known as AI.¹²⁸ Several of the acquisitions since 2000 have failed, in some cases causing successful companies to close down entirely. This can be due to poor strategy on the behalf of the acquiring company, as in the case of of the chip manufacturer TTP Communications, acquired and closed by Motorola.¹²⁹

Foreign acquisitions pose a number of other risks. Research and development funding may be reduced, although academic literature tends to dispute this. However, there is a consensus among economists that takeovers do not on average make money for their buyers. There are many possible reasons for this. The nature of innovation changes once a company is taken over. New owners tend to be more concerned with what businesses already do, rather than leveraging what they know.¹³⁰ There are risks to a firm's culture, for example; once owned and locked into a multinational structure, a business is much more constrained and tends to be less innovative.

If takeovers are risky, it is also true that they are less risky when a company is skilled in absorbing other companies. Many of the tech giants have a well-developed takeover strategy. However, takeovers are not straightforwardly about increasing profits and value of company that is bought. The expertise and staff may be the real target; or market share, or a desire to eliminate competition in a

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

particular part of a market. Many takeovers of UK companies centre on key aspects of emerging digital tech.

Sometimes takeovers may be about defending or controlling patents; this was the motivation for Microsoft to buy Nokia's Devices and Services arm,¹³¹ and for Google to buy Motorola.¹³² Both wanted to be insulated from patent claims as they developed mobile technologies.¹³³ 'Patent' takeovers lack motivation to improve the economic activity of the company that is bought.

Takeovers may be in the interest of a US owner, but are less likely to be in the interests of the UK economy. Once acquired, companies will generally restructure to ensure their profits are located overseas to minimise corporation tax.¹³⁴ For example, ownership of intellectual property, trade marks etc, can be moved offshore, while the UK subsidiary pays to use them,¹³⁵ and changes can be made to the company's structure so that the UK company pays its parent for services, reducing UK 'profits' and therefore corporation tax.¹³⁶

A common reason put forward for takeovers is that UK companies lack the ability to 'scale'. Few European tech companies have become global players, and even fewer have established dominance.¹³⁷ On the other hand, there are many UK and European Open Source and open technology success stories, including Raspberry Pi, Linux; the web was developed by a European.

However it is questionable whether US takeovers really lead to UK tech companies scaling up. Nevertheless, it appears to be an accepted but unstated policy goal that UK tech start-ups are aiming for US investment, or to be bought outright by a US company.¹³⁸

SECURITY RISKS

Security in a vendor's systems relies on the vendor and therefore on contract. Vendors themselves often cascade this responsibility to other vendors who supply components. While law and policy attempt to deal with this complexity through measures such as the EU's NIS regulations, and the UK's Cybersecurity and Resilience Bill,¹³⁹ dealing with vendor software is inherently opaque. Government employees do not typically have access to vendors' code, nor can they modify it or fix bugs; governments may compel access, but such powers likely to be exercised on an exceptional basis rather than as a routine matter.¹⁴⁰ On the other hand, when UK government employees need problems fixed on the government's web estate, they have full access and control,¹⁴¹ and can pick any

TECH GIANTS AND GIANT SLAYERS

vendor they wish, because the code has been developed by the Government Digital Service (GDS) as an Open Source resource.

While Open Source also has security challenges, particularly that it is vital to ensure that code used is properly maintained, there is an ongoing debate about whether Open Source software might be inherently more secure, due to the transparency of code. The literature is inconclusive; it is very difficult to measure 'security'.¹⁴² It appears to be true that incentives to improve open code ('bug bounties', or rewards to security researchers to report security vulnerabilities) can be an effective way to improve security.¹⁴³ In any case, the use of Open Source is so pervasive in closed systems that it is probably unhelpful to discuss whether one is better than the other; it is essential to recognise the importance of ensuring that Open Source technologies used in government systems are properly maintained and secure (see the discussion at *Strengthening Open Source*).

POLICY RISKS

We have already implicitly recognised the potential for foreign policy leverage, which comes from excessive and inadequately managed dependence on US tech.

VENDOR-LED POLICY MAKING AND TECH SOLUTIONISM

Vendors press for policies that suit themselves. They emphasise the need for the UK to be 'attractive', meaning low tax, low regulation and low intervention. It is easy to see that such policies are likely to be self-defeating, as in the long term they undermine the foundations of the economy, including trust, education, and infrastructure, but it's harder for politicians to resist when they are desperate for inward investment. In recent years, the tech lobby has pressed hard to halt AI regulation, limit data protection, and reduce the impact of competition law.

There is a huge public appetite for independent regulation of AI and its risks.¹⁴⁴ The Labour government promised an AI Act,¹⁴⁵ which it later reduced to lightweight legislation that would support innovation.¹⁴⁶ Now, no general legislation is planned at all.¹⁴⁷ Incidents such as that surrounding the Grok image generator's 'nudification' feature reinforce the need for AI risk management, but are now being tackled as one-off issues¹⁴⁸ rather than systemic risks that result from the way that companies desire to apply the technology.

As for regulators, lobbying has shifted the legal powers and approach of the Information Commissioner, as we discuss at *Data protection*. Efforts to restrain

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

competition law have been particularly brazen. The Digital Markets Unit has investigated cloud lock-in, Google's ad market, and other problems in digital markets, causing the CMA to become a lobby target, as we discuss below (*Competition policy*). There is now pressure from big tech to remove 'opt out' complaints at the Competition Tribunal. This is ahead of a number of cases which would challenge some of the big tech abuses being suffered by UK customers (see discussion below, *Competition and Appeals Tribunal*).

There is another aspect to vendor-led policy making. Cash-strapped politicians are always looking for ways to cut costs and create efficiencies, as well as quick solutions to social problems. This often makes them an easy target for vendor claims about the new technologies' capabilities. Where vendors and their technology are already embedded into systems, their claims can seem even more attractive, as adding new features to solve new issues becomes simply a question of paying a bit more money. This can lead down a road where technology companies are driving the policy agenda,¹⁴⁹ for example, in justice,¹⁵⁰ borders, policing, benefits, health and education.

ONLINE POLITICAL DISTORTION

The potential for harms from social media is widely recognised and discussed. The answer put forward in the UK is direct regulation of access, content and moderation aimed at the platforms that pose high risks to children or society.¹⁵¹ However, it is very difficult to make this strategy work. For a start, it depends on the actors causing the problem to solve the problem. Secondly, it does not tackle the reasons that those platforms produce risks. Thirdly, it is vulnerable to lobbying from the platforms themselves.

Given that users do not want unpleasant experiences and false content, we might well ask why platforms prioritise these for many users. In the early years of the Internet, small forums would simply die if they did not eject bullies and liars.¹⁵² Today, such negative behaviour can thrive because the posters are not easily found and isolated on these vast platforms whose owners regard moderation primarily as a cost rather than a necessity. Meanwhile, other users find it nearly impossible to choose to live outside of the large platforms. Users are also locked into abusive relationships with these platforms, because they lack control over the content and intrusive advertising pushed on them.

TECH GIANTS AND GIANT SLAYERS

The turn of X and Meta to favour extreme right wing content appears to be politically motivated, either to placate Trump, or because this reflects the actual world view of their owners. Breaking their power requires action beyond regulation of their worst aspects. Instead, we need to break the abusive relationship, and let users define their preferences, and ultimately to escape to better platforms without cost, as ORG outlined in our report on platform accountability.¹⁵³

APPROACHES TO DELIVERING SOVEREIGNTY

No approach to Digital Sovereignty will ever remove all risks. In order to manage the risks and gain the rewards, thought must be given to identifying approaches that reduce the worst or most acute risks, or give the greatest benefits and are most achievable within a reasonable time frame. This explains the investment in European Large Language Models (LLMs), and desktop collaboration software in Germany and France. The former offers large economic benefits, while the latter helps resist short term threats, offers easy cost savings by opening a closed market, and is relatively easy to achieve as the software already exists.

We can compare some different approaches to Digital Sovereignty and risk management to illustrate how risks are managed in practice. These concentrate on software on which the UK government directly depends. (See *Appendix III Sovereignty risk management* for more detail.)

BUY PROPRIETARY BRITISH

Using UK systems that are reliant on proprietary technologies may seem like a potential mitigation, but British firms suffer the risk that they will be bought by US tech giants, which is frequently their goal. The Dutch government found themselves in this predicament to their cost when native cloud provider Solvinity was sold to the US company Kyndryl; the Dutch government had entered into contracts with Solvinity precisely to mitigate legal risks.¹⁵⁴ Reliance on proprietary technologies makes some risk mitigations vendor-dependent, and does not by itself address cost and lock-in issues. While interoperability can reduce lock-in risks, there are always exit costs, and vendors will tend to find strategies to encourage lock-in; it is always a risk with proprietary, non-transferable products.

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Compared with investing in Open Source, buying proprietary British products also produces less economic value overall, because open technologies are used and adopted more quickly by others. 'Buy Proprietary British' could risk a form of 'digital nationalism' and reduce the UK's ability to benefit from new technology developed outside of the UK.

SOVEREIGN CLOUD

'Sovereign cloud' initiatives from US vendors attempt physical and legal air gaps, but cannot fully mitigate all of the risks. Software remains in the control of a vendor, and foreign laws can still potentially cut long-term access to services even if the vendor is a licensee independent of the developer, as with Thales and Google's sovereign cloud offering.¹⁵⁵ By framing sovereignty in a narrow legal and technical sense, or as 'Sovereignty as a Service', big tech diverts attention from the fundamental problems with vendor lock-in.¹⁵⁶

IN-HOUSE SOFTWARE

Software that is run in-house, built with private sector contractors but fully owned and controlled by the government, can minimise some sovereignty risks such as long-term control.

So long as government uses or develops capacity such as that held by the GDS, this approach will typically cost more in the short term, but less in the long term. It can make sense in cases where government systems must be bespoke, but it misses the benefits of sharing code onwards with the private sector and other governments.

THE DIGITAL COMMONS: OPEN TECHNOLOGIES

Most tech companies operating at scale are not prepared to take the same risks as government by accepting fundamental dependence on others. This does not mean they develop all of their software in-house. Rather, they decide which parts of their software stack are best developed with others as Open Source projects. An estimated 77% of code within proprietary products is derived from Open Source projects.¹⁵⁷ Proprietary elements define competitive advantage, while Open Source collaboration cuts costs.¹⁵⁸ Open Source is also used commercially to push competition and innovation in ways that suit the distributor. For example, releasing Open Source software that competes directly with a rival can force the competitor to yield market share or lower its prices.¹⁵⁹

TECH GIANTS AND GIANT SLAYERS

Most of the largest tech companies rely on Open Source software to deliver cloud and AI systems, including Linux at the operating system level, web servers like Apache, and so on, and develop Open Source in ways that tend to reduce costs overall. This protects multinational tech vendors from the worst risks of vendor dependence, such as cost hikes, especially at an infrastructure level. Such advantages can be also be leveraged by government, if desired, especially in collaboration with other governments, to shape the market and increase sovereignty and autonomy overall.

The challenges with open technologies include a greater requirement for expertise and drive, and the fact that most current systems are proprietary, so change is potentially a massive task. Pragmatic judgements about where and when Open Source is appropriate are required in practice, matching the strategic advantages to prioritise where to change, and where to accept the pain of living with closed systems.¹⁶⁰ Understanding the skills, costs and need for coordination structures is critical for success.¹⁶¹

EUROPEAN AND INTERNATIONAL COLLABORATION

Using open technologies can be combined with international collaboration. With off-the-shelf technologies such as Linux for server or desktops, this is implicit. Leading commercial Linux providers, which would be needed for support, are based in the US (Red Hat/IBM),¹⁶² Germany (SUSE)¹⁶³ and the UK (Canonical/Ubuntu).¹⁶⁴ Any of these can potentially be chosen without sacrificing sovereignty, as software deployment options are more flexible.

Projects like OpenEHR¹⁶⁵ for health records and software, in which the UK is a participant, X-Road¹⁶⁶ for government data records and access, and Matrix¹⁶⁷ for secure messaging, have collaborative processes for governments and developers to work together to reach their common goals. Far from creating autarky, these models create open markets and international competition while ensuring governmental autonomy and control over their systems. We explore these examples further in *Part III Beyond the UK*.

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

PART II
CURRENT UK POLICY POSITION

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Digital Sovereignty is a strategic issue but is noticeably absent from public UK policy documents. At the highest level, acute risks to Digital Sovereignty, such as close downs, sanctions against individuals or compelled backdoor access to government data, are not listed in the public version of the 2025 National Risk Register.¹⁶⁸ However, some of the underlying “chronic” risks are listed, particularly: “Impacts from reliance on digital platforms and digital services for services and interactions”; “Concentration of risk through dominance of global tech” and “Impacts from use and capability of artificial intelligence (AI)” ; and “Impacts from the use of end-to-end encryption”.¹⁶⁹

The National Risk Register says that these chronic risks are managed through a: “methodology [which] utilises futures and systems thinking¹⁷⁰ to help policy makers understand their implications and develop appropriate mitigations. The full analysis is currently an internal, classified document.”¹⁷¹ It is very concerning that this analysis and mitigation strategy is currently classified information, excepting a very brief overview in the Chronic Risks document.¹⁷² We discuss the risks of this closed analysis in more detail below at *Systems thinking and UK Digital Sovereignty*. Some European governments have made much more detailed analysis and discussion publicly available.¹⁷³

The 2025 UK Industrial Strategy notes:

As the world navigates a period of upheaval – driven by great power competition, climate instability, migration, and demographic transitions – the Industrial Strategy must not only stimulate economic output, it must help the UK adapt, compete, and endure.

Upheaval in geopolitics is also colliding with the emergence of advanced AI. The superstar firms of 2035 will leverage AI, just as other general-purpose technologies such as steam or electricity were harnessed by the superstars of their day. The Industrial Strategy builds on the AI Opportunities Action Plan to make the UK an AI maker rather than an AI taker, developing Britain’s stake across the AI value chain.¹⁷⁴

The contrast with European countries is stark. Risks to sovereignty include loss of access to core AI technologies, over-dependence on US information technology in general and supply chain risks to the chips needed in manufacturing. These risks are the subject of specific and openly discussed strategies being implemented at EU level, and more substantively in Germany, France, Netherlands, Denmark and

TECH GIANTS AND GIANT SLAYERS

other countries, who have all taken significant steps towards addressing the risks.¹⁷⁵

THE GROWTH AGENDA

The current administration identified the tech sector as one of eight key sectors, in a ten-year plan designed to turn around long-standing low productivity and growth. The Modern Industrial Strategy aims to make the UK the “best country to invest in anywhere in the world” and states that it wants a “whole-government effort” that looks for the state to play a more active role in the economy.¹⁷⁶

The strategy has been criticised as private-sector led, placing the public sector as facilitator while expecting private sector investment to finance economic change.¹⁷⁷ In comparison with other countries, including US policy from the Biden presidency, or Germany, France and the EU, the UK government is playing less of a direct role.¹⁷⁸

The strategy also claims to be ‘place based’, meaning that local connections for delivery are critical for growth. The strategy recognises the importance of this for the tech sector, but the highly centralised UK state may not have the capability to engage effectively in this way.¹⁷⁹

At the level of the Tech Sectoral Plan, the strategy discusses cybersecurity, and develops the government’s approach to AI, but focuses on private sector growth without fully developing the theme of “upheaval in geopolitics” and how the UK might “adapt, compete and endure”. It does not ask how the UK can secure a sovereign infrastructure or whether government spending is in fact working against the IT sector’s and UK economy’s interests, nor does it discuss the resulting cybersecurity risks.¹⁸⁰

Plans for AI adoption through the UK economy are driven by the AI Opportunities Action Plan,¹⁸¹ and operationalised through the UK-US Tech Prosperity Deal. These partnerships are with large American corporations such as Microsoft,¹⁸² Open AI,¹⁸³ Google DeepMind,¹⁸⁴ Anthropic¹⁸⁵ and Oracle.¹⁸⁶ The main strategy is support from and for US tech, in the hope it will deliver benefits but with the inevitable result that they will extract significant value from the UK economy.

DSIT has established a Sovereign AI Unit, the one area where the idea of ‘sovereignty’ is placed in plain sight. The main risk it identifies is a lack of

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

“compute”, meaning that the main thrust of the strategy is building data centres capable of provisioning mostly US-owned companies to sell their products to the UK. While the Tech Sectoral Plan does identify opportunities for UK AI firms and expertise are identified, it does not discuss the risks of dependency on US tech.¹⁸⁷

COMPETITION POLICY

The UK has led the way on competition policy, experimenting early with Open Banking to force open data exchange (interoperability) between digital financial services. Over 16 million users now benefit from Open Banking-based transactions.¹⁸⁸ Sweeping powers to impose obligations on dominant digital players were brought in through the 2024 Digital Markets, Competition and Consumers Act (DMCCA).

However, big tech investors raised concerns over the possibility that tough measures would be imposed on them. Doug Gurr, a former Amazon UK and China executive, was appointed the interim chair of the CMA in January 2025, after Marcus Bokkerink stepped down after just two years of a five-year term. Chancellor Rachel Reeves explained that Bokkerink, “recognised it was time for him to move on and make way for somebody who does share the mission and the strategic direction that this government is taking”, referring to the growth agenda and emphasis on AI adoption.¹⁸⁹ The Open Markets Institute, an anti-monopoly thinktank, called the move a “strategic blunder”.¹⁹⁰

The UK government issued a “strategic steer” to the CMA in May 2025.¹⁹¹ This stated that the CMA should be “prioritising pro-growth and pro-investment interventions”, and should “take particular care to collaborate with all interested parties to ensure growth and innovation benefits are prioritised, including through supporting the government in delivery of the AI opportunities action plan”. This appears to signal that the UK did not want the CMA to take any actions that might discourage big tech investments in the UK, particularly in cloud and AI infrastructure.

STRATEGIC MARKET STATUS AND EX-ANTE OBLIGATIONS

Firms can now be given “Strategic Market Status” with the expectation that market correction measures such as interoperability requirements will be imposed. Google was so designated in 2025 for its dominance of the online ad market,¹⁹² while Google and Apple were both so designated for holding a duopoly in the mobile market.¹⁹³ A CMA investigation has found that Amazon Web

TECH GIANTS AND GIANT SLAYERS

Services (AWS) and Microsoft hold a combined market share of 70-80% in the UK cloud infrastructure market, and has identified egress fees, restrictive licensing practices and technical barriers as their means of restricting competition. The CMA investigation report recommends that they are designated as having Strategic Market Status.¹⁹⁴

However, the test of designation is whether appropriate duties are imposed on companies that are given SMS status. There are signs that the obligations the CMA is choosing are extremely cautious. Proposed obligations on Apple regarding their App store have been widely held to be effectively a commitment to consult with third party publishers, while Apple are allowed to place barriers on developers, such as charges for the use of their Application Programming Interfaces (APIs). Open Web Advocacy say that:

Apple retains extremely broad discretion to reject interoperability requests while remaining in full compliance, meaning the gatekeeper still decides how much competition to allow proposed measures

and conclude that the CMA's obligations:

would leave in place the kind of anticompetitive conduct that the DMCCA was specifically passed to address, to the detriment of both UK consumers and UK businesses.¹⁹⁵

A charitable reading of the CMA's approach would be that they are being cautious before moving more swiftly, but their prior investigations should be read as strong evidence of the urgent need for action to resolve the abuse that they have already found.

COMPETITION AND APPEALS TRIBUNAL

Big Tech is applying further pressure on competition policy regarding opt-out claims brought to the Competition and Appeals Tribunal (CAT), according to former digital minister Damian Collins OBE and the Competitive Britain campaign.¹⁹⁶ A call for evidence in 2025 has opened the question of whether these should be abolished.¹⁹⁷ The major beneficiaries of abolition would be big tech companies, as many digital competition harms are very large in scale, but impact individual consumers by relatively small sums. This means it is hard to gather them together in opt-in claims. Several important digital claims are currently progressing at the CAT under the opt-out process. Microsoft has been challenged

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

for charging more for their licenses when their software is deployed on competitor's cloud.¹⁹⁸ If successful, this could open up the cloud market significantly. Another case against Meta, would force Facebook to stop demanding to aggregate user data across its platforms, a policy that forces users to accept massive privacy invasions.¹⁹⁹ A third targets Google for abusing its dominance in the adtech market, and preferencing its own products.²⁰⁰

MERGERS AND ACQUISITIONS

Mergers and acquisitions are important for Digital Sovereignty because they help keep the market competitive and because strategically important companies can guarantee some degree of interdependence between the UK and other countries. Mergers and acquisitions can be blocked either on competition or national security grounds.

The UK has been relatively unconcerned about the foreign acquisition of UK companies since the 1980s.²⁰¹ Nevertheless, there has been enough concern to generate new powers to block strategic assets from being sold. The National Security and Investment Act 2021 allows sales to be blocked on national security grounds. The TBI objected that the powers are unclear, and stated that “there is no clarity on when and how the government might deploy them or, most importantly, the framework through which it will assess national security concerns”. A government consultation in August 2025 promised “sharper definitions, more guidance, new exemptions and greater transparency”.²⁰²

The UK's policy position on national security is less restrictive than the approach in France and Germany. France examines takeovers, acquisitions and significant holdings in “critical technologies”, which is likely to be expanded to include AI and quantum computing. This matches France's wider ambition of strategic autonomy.²⁰³ German laws require notification in 27 sectors, including “autonomous driving, robotics, AI, semiconductors and components, quantum technologies, nuclear materials, 3D printers, smart metering gateways, certain telecommunication or surveillance products”. Germany is currently reviewing its legal powers.²⁰⁴

The results of pressure on the CMA have already been stark. In 2025, no merger on competition grounds was blocked, the first time since 2017 that every merger has been cleared. The CMA has stepped back from intervening in international mergers where the UK is not as central. The government is also considering

TECH GIANTS AND GIANT SLAYERS

revising the way merger requests are handled, potentially moving them away from an independent panel, and placing the duty under a committee of the CMA board.²⁰⁵ The implication is that mergers will be evaluated with greater political direction.

We look at the impact of mergers and acquisitions below, at *Impact of UK tech companies being sold to tech giants*.

DATA PROTECTION

The Information Commissioner's Office (ICO) has been given a legislative duty to balance enforcement with business innovation. Recently, it consulted on means to reduce its obligation to enforce data protection;²⁰⁶ it has been called out for its generally poor record of enforcement.²⁰⁷ While the UK data protection framework achieved adequacy agreement with the EU, allowing mutual recognition of standards and easier data flows with Europe, the EU was worried about the potential that statutory instruments could quickly water down the rules. This executive power invites lobbying for further exemptions with minimal democratic oversight.²⁰⁸ The EU Commission has retained the right to call in future SIs for rapid review should they appear to impact EU residents' rights.²⁰⁹

SOCIAL MEDIA POLICY

The UK government currently distributes commentary and updates almost exclusively through the dominant platforms, especially X, Facebook, Instagram, Threads, YouTube and Tiktok. A small amount of content can be found on smaller platforms such as Flickr. Content production and advertising spending from government also flows to these American platforms.

Elsewhere, the UK government seeks to regulate the same platforms, and Parliamentarians likewise worry about the impacts of social media on society. The disjunct between the theory and practice of government could not be more stark: on the one hand government reinforces the monopolies of the dominant platforms, including through monetary payments, and on the other it legislates against their ill-effects. Proposals to regulate the Grok AI chatbot with specific legislation on AI-generated image content reflect this focus on the most extreme problems that emerge from digital systems rather than regulating to shape the dynamics within the systems.²¹⁰

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

UK legislation and regulation is inconsistent. Concentrating on content regulation alone relies on businesses whose interest in user attention and low moderation costs directly conflicts with the objective of user safety. It is in effect legislating for better oligarch behaviour. A more strategic approach would use competition and data protection enforcement to change the market dynamics. If platforms' interests can be realigned with users' interests, costly and controversial social media legislation could be more limited in scope and have greater chance of success. This approach is outlined in ORG's report on platform accountability.²¹¹

The social media and online advertising market is a clear case of duopoly, with Google in a very dominant position across search and website ad placements, followed by Facebook within its own platform. Social media's use of personal data, especially in advertising, has long been unlawful, and also generates the market dynamics behind online harms.²¹² Despite the obvious harms, regulators have been under pressure to deregulate. This summer, the ICO began work to legally permit aspects of cookie-based data sharing for advertising purposes. This significantly benefits the American tech giants.²¹³ They are also proposing to curtail their investigations to those they deem represent the greatest harm to the largest number of people, in apparent contravention of their statutory duties.²¹⁴

UK SPENDING ON DIGITAL TECHNOLOGIES

UK government spending on digital technologies stands at around £26bn a year, but is significantly lower than other similar countries.²¹⁵ The government State of Digital review in 2025 found that systems are under-digitised, and dependent on legacy systems. It identified significant productivity problems, cybersecurity risks, fragmented data systems as the results.²¹⁶

The National Audit Office (NAO) has criticised government digital spending for waste from failed or expensive projects: poor outcomes; excessive prices; embedded consultancies; lack of opportunities for UK tech SMEs; and vendor lock-in. The agenda for reforming government IT the NAO identifies is broadly similar to the fundamentals of the Digital Sovereignty debate. Government has insufficient control and management of its own digital tech, and incumbent vendors are calling the shots: "There is not yet a shared strategic approach across government to dealing with a few very large suppliers who now dominate technology markets".²¹⁷

TECH GIANTS AND GIANT SLAYERS

Both the NAO and the government's State of Digital review explain that there are problems with procurement, although the government review frames this largely in terms of volume discounts and benefits of scale without looking closely at vendor lock-in and the dependent relationships involved.

The State of Digital review and the NAO highlight dependency on external expertise and institutional capacity as root causes of failure. The NAO also noted that the Government Commercial Function had 6,000 employees but only 15 digital experts to deal with their 19 largest digital suppliers.²¹⁸

VENDOR LOCK-IN

The NAO explains that “every major operational system, from borders to tax to welfare, depends on the successful performance of its suppliers” but has warned that digital services are increasingly “subscription-based” and government “does not ultimately control” them.²¹⁹ This problem is particularly acute when specific vendors supply operating systems, cloud or other fundamental systems, as they cannot be easily swapped out for competitors' products. Those vendors currently dominate the market.²²⁰ The difficulties of avoiding cloud lock-in are recognised by the government, whose policy is to balance risk and value, particularly by avoiding tie-in to long term deals, and speeding up delivery.²²¹

There are long-standing measures to reduce vendor dependency, including UK policies to promote Open Source and Open Standards.²²² Both approaches have been favourably identified in both Labour and Conservative administration policies since at least 2002.²²³

Open Source has proven results within UK government. In the 2000s, the UK government web presence was suffering from high costs and a poor user experience. The GDS, set up in 2010, moved to using Open Source software for websites across government, reducing costs and improving ease of management. Government websites in Israel and New Zealand have drawn on UK code.²²⁴

Government policy since 2012 supports Open Standards in software procurement,²²⁵ designed to ensure “equal access to government IT contracts for open source and proprietary software providers”, “avoid vendor lock-in to a specific piece of technology or supplier” and “reduce the overall cost of your digital service or technology programme”.²²⁶ If a service is based on an Open Standard then software can be swapped in or out along with its vendor. Open

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Standards can be supported by both Open Source and proprietary products. This forces competition up and prices down.

As of 2023, the UK's Digital, Data and Technology Playbook also recommends Open Source:

There is an expectation that government software and code is open-source by default. This means it should be developed in the open and published using an Open Source Initiative (OSI) approved licence. Open and interoperable software will enable:

- transparent and clear documentation, making it easier for teams to maintain the code, understand the data, track changes to the code and data and for other people to use the Application and data
- reuse of software components built by others
- reduction of overall cost of digital services or technology programmes²²⁷

Exemptions and exceptions within this policy are used to continue buying proprietary technology such as cloud procurement. The rush towards AI technologies is causing a failure to examine whether proprietary technologies are the right choice. Procurement should rigorously adhere to the principle of interoperability so that AI models and vendors can be swapped out and replaced. Cloud interoperability would now need to be imposed on the vendors, for example through competition law.

There are signs that Open Source policies may be being quietly removed or rolled back. The NHS removed Open Source policies from its websites in mid 2025.²²⁸ At the Ministry of Defence (MoD), the preference for Open Source procurement at Commercial X was reversed²²⁹ after pressure from SMEs who wanted exclusive rights in order to resell capabilities they had devised, arguing the move would provide greater economic benefits.²³⁰ This assumption runs against research findings that open access to technology spurs further and wider innovation, producing four times the economic value of the original outlay.²³¹ The SMEs' preference for proprietary commercialisation appears to have been accepted without fully considering the ramifications for MoD technological dependency or whether UK economic growth might be better served by the earlier policy.

TECH GIANTS AND GIANT SLAYERS

Palantir's introduction into the NHS and Ministry of Defence offers a salient example of how Digital Sovereignty can be sacrificed and vendor lock-in swiftly completed.²³² Palantir introduces core systems to manage data, which are proprietary. Any further components must use the company's tech. Palantir is then best placed to build additions, which further excludes competition.²³³ The MoD was warned in its own research, commissioned from Rand:

there are risks such as vendor lock-in, or reliance on foreign suppliers of AI systems or related services (e.g. compute or secure Clouds) that constrain a country's freedom of action and security of supply.²³⁴

UK AND CLOUD SUPPLIERS

A key part of the UK's strategy to reduce dependence on problematic IT vendors has been to shift away from using on-premises hosting towards using cloud providers. This approach, introduced in 2013 and called 'Cloud First',²³⁵ is supported by the G-Cloud digital marketplace, which helps with deployment and management.²³⁶ G-Cloud has advantages such as reduced maintenance costs and easier management, as the infrastructure itself is managed. However, combined with failing to encourage domestic alternative providers and allowing a major UK provider to be sold to a US cloud provider, the result is over-dependency and vulnerability to price hikes, as the government's own analysis has itself recognised.²³⁷ Efforts have been made to reduce escalating costs, for example at the Home Office, but they do not remove the underlying dynamics.²³⁸

Cloud pricing at Microsoft is rising fast as the company attempts to recoup its cloud and AI investments.²³⁹ Microsoft first moved its customers onto a cloud-based system and then introduced its 'Copilot' integrated AI. Furthermore, Microsoft deliberately makes it prohibitively costly to run its software on non-Microsoft cloud systems. The company says business prices rose by 10-20% in 2022,²⁴⁰ or 20-40% by some independent calculations,²⁴¹ followed by 9% in 2023,²⁴² a mix of increases and reductions in 2025,²⁴³ and increases of 4-10% scheduled for July 2026.²⁴⁴ The CMA finds that the UK is being overcharged by at least £500m a year in the cloud market.²⁴⁵ The Social Market Foundation estimates government will be overcharged by at least £300m over this Parliament through restrictive software licensing conditions.²⁴⁶ Analysts note that domestic users facing 30% increases in Copilot fees in 2025, and this rise is likely to come to commercial licences in future.²⁴⁷

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

The government's recent interventions at the CMA to reduce interventions will only exacerbate the state's vulnerability to price hikes and overcharging.

Interoperability and unbundling requirements would create competition and downward pressure on pricing for the UK government as well as businesses. Instead, government has undermined competition mechanisms to reduce dependency, leaving it with no clear means to reduce over-pricing, except through bulk buying arrangements.

UK STRATEGIC SUPPLIERS

Nearly all of the government's major IT vendors have long been identified as strategic suppliers, and have also been the subject of controversy. AWS and Microsoft are both subjects of current criticism and investigations for anti-competitive practices and over-pricing.²⁴⁸ Oracle is notorious for being incredibly costly to remove once systems have been built using their software, for being costly while using deliberately opaque contracts, and for squeezing commercial customers through aggressive licensing checks.²⁴⁹ Two of the suppliers are consultants Accenture and Capgemini, whose repeated failures and cost overruns led government to try to terminate its relationships with them in 2017. HMRC found them and their technology partner, Fujitsu, impossible to replace due to their embedded knowledge.²⁵⁰

Government has also recognised problems with Capita, and attempted to move provision of software services to cloud providers, but recognises this just traded one set of vendor lock-in problems for another.²⁵¹

On the positive side, IBM's contracts include supplying Open Source cloud management tools, reducing vendor lock-in risks. However, many of IBM's products are proprietary, including the asset management tools used by the MOD, and its partnership with Oracle does not avoid lock-in to Oracle products.

See *Appendix IV UK tech strategic suppliers* for more detail on the failures and over-pricing observed from these companies.

TECH GIANTS AND GIANT SLAYERS

Direct revenue spending on strategic suppliers 2024-5 ²⁵²	
UK companies (incl Capita):	£1.1bn
US corporations in 2024-5:	£1.3bn
Other non-UK (CA, IE, FR, JP)	£3.1bn
Total spend:	£5.5bn

WHY IT PROCUREMENT FAILS IN THE UK

IT procurement in government is difficult, even without having to grapple with companies' desire to create long-term dependence.²⁵³ There are few available major contractors, and legacy systems are often maintained because of the complexity of replacing them.

Government is operating in an uncompetitive market, which it often recognises implicitly by not taking work to tender because the existing arrangements preclude choosing any other partner.

It is this lack of a competitive market that requires government to change course to rely on control of its own code and enforce interoperability through Open Standards and ensure that it does not become a victim.²⁵⁴ Enforcing these strategies requires institutional strength and political commitment.

GOVERNMENT DIGITAL SERVICE

While UK progress towards better digital procurement has been partial and sporadic, there are some good examples, mostly driven by the GDS. In 2010, the UK was among the first governments to establish a strategic centre of IT expertise – the GDS. This approach was copied by a number of other countries, including Canada, the US, Australia, New Zealand, Finland, Italy, Argentina, Singapore, and Uruguay.²⁵⁵

GDS's major successes include modernising the government's web estate and making the software behind it available to the public. GDS also in-sourced the DVLA's software systems, which had been fragile and expensive. The "Partners Achieving Change Together" consortium (PACT) included IBM, Fujitsu and the consultancy Concentrix, and cost £230m a year. Around 400 staff and 300

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

contracts were brought back in-house.²⁵⁶ Some of the code is now published as Open Source software. Costs were cut by 19% per year.²⁵⁷

GDS drove these policies for Open Source and interoperability, with good results. For example the NHS now has an interoperability program to ensure systems work better with each other, adopting Open Electronic Health Records (OpenEHR) as the standard for patient records, potentially allowing it to replace software components.

By 2018, GDS's momentum had slowed in the face of departmental resistance to another part of government taking management of their systems.²⁵⁸

NHS AND PALANTIR, OPENSAFELY AND OPENEHR

OpenSafely is UK success story in a particularly difficult area, the use of NHS patient records for medical research. The potential for research access and need for reproducible results has to be balanced with the privacy of individuals.²⁵⁹ The platform is a “a secure, transparent, open-source software platform for analysing electronic health record data. All platform activity is publicly logged. All code for data management and analysis is shared under open licenses and, by default, for scientific review and efficient re-use.”²⁶⁰

Organisations such as medConfidential, the BMA, and the Royal College of GPs gave their support to the system, where previous attempts had failed. The project's governance includes a wide group of stakeholders.²⁶¹ The project was conceived during the COVID pandemic.²⁶² Also for COVID research purposes, later, Palantir persuaded the government to adopt its own more intrusive technologies by offering them at a loss, hoping for more profitable adoption in future.²⁶³

OpenEHR has been an international success, with wide adoption in Germany, Netherlands, Sweden and Australia, as well as the UK. It aims “to combat the fragmentation of clinical data, which has historically impeded effective healthcare analytics and AI applications” and has begun to have significant market impact. Gaps in adoption remain, however, limiting its value to the NHS as a whole.²⁶⁴

Palantir's systems appear to be pitched at dealing with the difficulties with performing analytics on disparate datasets.²⁶⁵ In giving Palantir the contract for the entire NHS Federated Data Platform, the NHS has placed the company at the

TECH GIANTS AND GIANT SLAYERS

centre of its data systems. This is precisely the kind of decision which creates risks of long-term vendor lock-in.

WHY IN-SOURCING AND GDS HAVE STRUGGLED

Mike Bracken, GDS's founding executive director, points to difficulties with the Treasury, which lacked understanding of what GDS were trying to achieve: "Alignment with the Treasury was probably the biggest single problem we had in GDS". This is likely to be related to Treasury spending controls, and the unpredictability of software projects. The Treasury is frequently felt to favour 'soft PFI' spending.²⁶⁶ If a large IT investment is made by an outsourced contractor, the Treasury does not need to approve the investment costs, which would otherwise have to meet complicated meeting fiscal spending rules. Instead, the UK overpays the contractor over a period of years.²⁶⁷ The result is that the private company owns the software assets, and achieves vendor lock-in.

Other departmental rivalries also blocked attempts to provide cross-departmental functionality:

Some of the GDS's greatest achievements, Bracken believes, were won despite – not because of – the civil service's structures and culture. The GDS and the DVLA's digital teams, he said, were able to transform the agency's services – whilst cutting operating expenditure by 19% in two years – because "nobody was looking! Swansea is a long way away, and they had a very good permanent secretary who let them get on with it. But that was the exception".²⁶⁸

Bracken points to the need for high-level political buy-in. The story also demonstrates the requirement for planning capacity in central government, so that strategic needs and implications can be better baked into policy.²⁶⁹

MODERN DIGITAL GOVERNMENT AND THE COMMERCIAL DIGITAL CENTRE OF EXCELLENCE

The government's "blueprint for modern digital government" was set out in January 2025, and reflects the concerns identified by the NAO, for example improving leadership. Many of the suggestions are sensible, such as ensuring there departments make APIs available. Central to this plan is the creation of a Commercial Digital Centre of Excellence at DSIT.²⁷⁰

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

The government says this body will in future answer NAO concerns about managing relationships with vendors and making better decisions about when to build and when to purchase from vendors:²⁷¹

There is no mention of collaboration with other governments and the potential for technology sharing through shared projects.

However, the plan for Modern Digital Government does not mention Open Source or Open Standards or their benefits. Vendor lock-in is mentioned only briefly. There is no mention of collaboration with other governments or the potential for technology sharing through collaborative projects. There is an emphasis on promoting the use of AI, but no discussion of how to manage the dangers it poses for vendor lock-in or Digital Sovereignty.

As yet there is no clear vision for how some cross-government projects might be managed. The document gives the impression that technical leadership will mostly be found within government departments. That is likely to be more difficult than leading with specific governmental organisations, similar to the UK's GDS, ZenDis in Germany, or other international examples we explore in *Part III Beyond the UK*, where technologies are stewarded by dedicated bodies, cooperating or even operating across borders.

AI PROCUREMENT

With AI procurement, it is less clear whether the issues around vendor lock-in are being properly considered. Research from Stanford shows that open weight models from the US, China, and Europe are now very close to the performance of proprietary models, which by some performance measures are within 1.7% of their closed competitors²⁷² and often offer better value, especially if customisation or greater transparency is needed.

There are sporadic examples of open weight models being used in the UK government, according to freedom of information research from the Social Market Foundation, who highlight the lack of clear policy and guidance.²⁷³

The Artificial Intelligence Playbook for the UK says to “consider strategies to avoid vendor lock-in” but does not expand further.²⁷⁴ Guidance on AI procurement is also thin on the topic, advising that ensuring ‘explainability’ may help avoid vendor lock-in if teams wish to turn to new vendors.²⁷⁵ The AI Playbook refers back to the UK, Digital, Data and Technology Playbook and the guidance in the

TECH GIANTS AND GIANT SLAYERS

Government and Technology Code of Practice, which specifically favour Open Source and interoperable approaches.

Given the pace of change, that guidance is now somewhat out of date. Modular approaches can help the government avoid tying itself to a specific vendor or model. Open Source tools have been developed to help deploy and manage different AI models. Open Source tools can act as an intermediary between IT systems and AI models; one tool built by France specifically for use in government allows models to be swapped in and out.²⁷⁶ Another tool from France's AI incubator allows blind testing to compare different AI models.²⁷⁷ The AI Incubator within DSIT is aware of these initiatives,²⁷⁸ but government guidance has not yet reflected the availability of tools to manage relations with AI providers.

DIGITAL SOVEREIGNTY BEYOND WHITEHALL

Unlike other countries, the goal of Digital Sovereignty is not defined or stated publicly at any level of government. However, there are projects which aim to reduce vendor dependency and costs.

LOCAL GOVERNMENT

Local government suffers from the same problems as national government, but has less capacity to co-ordinate. Spending on consultants as a whole has been rising, despite a decade of austerity.²⁷⁹ Among IT vendors, Oracle is one of the ones causing the highest-profile problems, with reports of price hikes and vendor lock-in. An Oracle procurement failure in which Birmingham council attempted to replace an SAP enterprise management system saw a £19m project reach £170m by late 2025,²⁸⁰ while in a similar project West Sussex found its cost escalating to 15 times the initial estimate.²⁸¹ Despite these repeated problems, Oracle recently picked up a third project of this type at Dorset,²⁸² indicating the lack of choice councils have for products of this kind.

Dissatisfaction with vendors for other core functions such as administering rates and benefits from companies such as Capita have led to efforts to create an Open Source alternative, Open Revenues and Benefits. It appears to have promise, but the effort is mostly the work of local councils rather than a result of central co-ordination. Exit costs from legacy systems are steep, estimated at around

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

£300,000 per council.²⁸³ The project leaders say the benefits of an Open Source approach are “deafening”. Despite the barriers, Leeds, Basildon and Teignbridge appear determined to lead this effort to shake off the legacy proprietary systems.²⁸⁴ Another project, Open Source IMS, is aimed at managing council income.²⁸⁵ Hackney developed software to manage adult social care, following a devastating cyber attack on their vendor’s proprietary system. Although Hackney’s software was not deployed permanently, the developers believe their Open Source approach would produce better financial and operational results.²⁸⁶

Policy efforts focus on procurement and collective purchasing difficulties, which are important, but do not focus on the root issue of vendor lock-in, which is about use of Open Standards and preferably Open Source. Local government needs to mandate Open Standards across markets, and ensure Open Source alternatives are built.

The Local Government Association has asked government for help to set up a Local Government Centre for Digital Technology, which aims at co-ordinating digital systems. The LGA believes this will work better than a central government facility, as it will be closer to councils’ needs.²⁸⁷ It will also bring councils together for projects to build new Open Source local government systems. The government’s response was to set up GDS Local, in which the LGA is a partner.²⁸⁸ GDS Local is looking at the requirements for local government, and where central government technology can help.²⁸⁹

With the help of the Convention of Scottish Local Authorities, Scottish local government has seen 23 of 32 authorities adopt the Open Source community management platform “Consul” from Madrid, driven by the requirement that 1% of local authority should be spent through participatory budgeting.²⁹⁰

WALES AND SCOTLAND

Scotland has had policies promoting Open Source and Open Standards since 2015.²⁹¹ Also in 2015, in the wake of the 2013 Snowden revelations, Commonwealth produced a paper arguing that Scotland’s Digital Sovereignty depended on the use of Open Source.²⁹² Scotland’s policy commitment to Open Source was reiterated in its 2021 Digital Scotland Service Standard,²⁹³ and the 2025 digital strategy vision statement states that progress in government digital services has been underpinned by “an increasing focus on collaboration and a greater focus on building re-usable solutions with best value across the sector.” However, the

TECH GIANTS AND GIANT SLAYERS

vision statement does not examine the value and use of Open Source and Open Source procurement to the digital economy, nor does it discuss the challenges of AI and cloud procurement.²⁹⁴

However, as with broader UK policy, these commitments may not have yielded the results that policy makers intended or desired, due to the same barriers of legacy code, resistant vendors and lack of internal leadership. More recently, Scotland has produced studies looking at the effectiveness of its IT systems and procurement, summarised in a report, *Foundations of the Digital State*. This report focuses on the need for state capacity to manage the process of digital systems development, both within government, including capacity to research future technology options and also within the Scottish Parliament, which needs sufficient knowledge to exercise oversight. It also looks at the role of digital technologies used to deliver legislation and also to shape the options available to government.²⁹⁵

In 2020, Wales created a Centre for Digital Public Services, analogous to GDS for the UK, and is currently planning to bring its capacities into the direct remit of the executive.²⁹⁶ Digital strategies include reference to interoperability and open data; and mention the use of Open Source “where possible” for health. However, a Transform Wales report sets out a more ambitious agenda, where Open Source could form a stronger basis for open government and local procurement.²⁹⁷

THE OPEN SOURCE ECOSYSTEM IN THE UK

The UK’s Open Source ecosystem provides a great deal of economic value, but lacks official support and encouragement. The UK leads Open Source contributions per capita, and is the fifth largest source of contributions globally.²⁹⁸ OpenUK estimates that it provides an estimated £13bn of annual value to the economy, or 27% of the total tech sector.²⁹⁹ While this estimate may seem surprising, it is echoed by international estimates of the scale of value created by Open Source. A 2024 Harvard study estimated the global demand side value of Open Source as \$8.8 trillion, meaning that “firms would need to spend 3.5 times more on software than they currently do if OSS did not exist”,³⁰⁰ and a study for the European Commission estimated that a 10% increase in Open Source contributions would add 0.4-0.6% to European annual growth.³⁰¹ The Linux Foundation has documented the return on its investment in contributing

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

organisations (of around 2-5x the investment, or up to 6x for organisations taking a leading role as members of Open Source software foundations).³⁰²

There are a number of globally significant Open Source SMEs in the UK including: Canonical,³⁰³ which supplies Ubuntu Linux; Collabora,³⁰⁴ which develops the Collabora online document editor; RaspberryPi, the educational tech developer and manufacturer,³⁰⁵ and Element, a French-UK company that supplies encrypted chat products to the Open Source world, European governments and NATO.³⁰⁶

There is no visible strategy to support, grow or make greater use of this economic activity that we could identify in government policy such as the Tech Sectoral Industrial Strategy.³⁰⁷ Open Source can be said to lack a marketing strategy, like many other public goods that people provide for the benefit of the community, rather than being marketed and promoted by high profile vendors. However, given Open Source's centrality to questions of Digital Sovereignty, economic development and dependency, and the leading role the UK has in Open Source, omitting it is unwise.

SYSTEMS THINKING AND UK DIGITAL SOVEREIGNTY

The problems underlying Digital Sovereignty risks are identified in the National Risk Register as “chronic” risks, including: “Impacts from reliance on digital platforms and digital services for services and interactions”; “Concentration of risk through dominance of global tech”; “Impacts from the use of end-to-end encryption”; and “Impacts from use and capability of artificial intelligence (AI)”. The NRR states that they are analysed in a *classified* document using “futures and systems thinking”.³⁰⁸

The government has published a very brief overview of its chronic risk analysis, but the summary gives little indication of the range of problems and mitigations identified, nor of their likely efficacy.³⁰⁹ It poses data protection and competition regulation as key example mitigations for the dominance of big tech, but has in practice reduced the effectiveness of these, as discussed at *Competition policy*, and *Data protection*.³¹⁰

The UK's civil service has taken an increasing interest in Systems Thinking since the 2000s in order to better understand complex problems, to produce more effective policy solutions, and to avoid unintended consequences.³¹¹ Demos' 2003

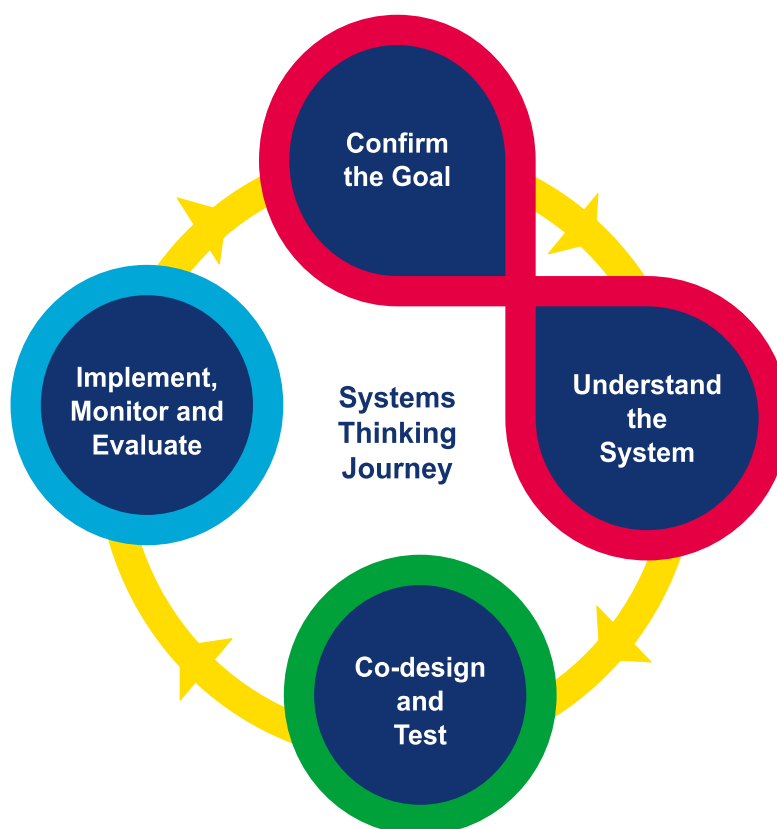
TECH GIANTS AND GIANT SLAYERS

book, *System Failure*, outlined the need for Systems Thinking in UK government.³¹² Examples of important Systems Thinking include Systems Engineering used for the US lunar landings,³¹³ and, at MIT, the seminal 1972 report “The Limits to Growth”, which used Systems Dynamics to produce a computer model analysing the interactions between humans and the Earth.³¹⁴

In 2020, the government’s Policy Lab introduced a toolkit to help civil servants consider “Government as a System”.³¹⁵ Sir Patrick Vallance, then Chief Scientific Officer and now Minister of State for Science, Innovation, Research and Nuclear, said:

It is vital that civil servants are able to confidently and effectively engage with the complexity and uncertainty inherent in the problems we tackle in government. Systems thinking approaches allow us to understand the full impact of interventions across department and policy area boundaries – ultimately leading to better solutions³¹⁶

The *Government As a System* toolkit offers a four-stage approach: Confirm the goal; Understand the system; Co-design and test; and Implement, Monitor and Evaluate.³¹⁷



THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

The toolkit presents information from Systems Dynamics, which looks at “feedback loops”. Other key concepts of Systems Thinking include the importance of “emergent properties” when “the whole is greater than its parts”. Digital platforms exhibit emergent properties such as network effects and lock-in, which in turn shape emergent behaviours such as patterns of online debate and abuse, and safety risks.

At the scale of the digital economy, emergent properties also arise. Network effects, data accumulation, economies of scale and platform intermediation produce systemic outcomes, including market concentration, attention-driven business models, platform dependency and infrastructure centralisation. As we have discussed in this report, these structural dynamics in turn shape downstream behaviours across society, from patterns of online debate and content production to the economic organisation of entire industries. Understanding what is in the system and what is not (the “boundaries” referred to by Vallance above) is therefore especially important for discussions of the “chronic” risks of Digital Sovereignty.

Political direction to exclude approaches, identify areas of concern or favour specific policy interventions can break the usefulness of systems analysis. The same is true of lobbying or pressure from the US to favour American companies, or the desire to avoid tariffs. If any of these excludes beneficial approaches suggested by a systems analysis of Digital Sovereignty risks, then analysis is of limited help.

Systems Thinking is a means to find best practice and unexpected ways of creating progress towards a goal. However, if the goal is purely political, Systems Thinking’s powerful identification of intervention points and means of shifting a system could become a sophisticated way of generating perverse results.

For example, the government is itself a generator of unhelpful feedback loops. Adding a new dependent vendor relationship with Palantir will generate new risks as the company becomes more embedded. Promoting US investment and lauding its success creates a cycle of further dependence. However, Systems Thinking could be employed to lower political resistance or find benefits within the plan of adopting new software systems. On the other hand, if Systems Thinking is used to pursue the wrong goals, it becomes corrosive and almost the opposite of a Systems Thinking approach.

TECH GIANTS AND GIANT SLAYERS

To resist such pressures and allow more intelligent policy debate, the government should publish its analysis of the digital chronic risk systems and their dynamics, including what it believes is 'in' or 'out' of a particular policy risk system. It is particularly concerning that the analysis of these chronic risks is classified.

It is also important that the civil service uses the full available range of Systems Thinking. Systems Dynamics, which the documentation appears to favour, is just one field of systems analysis among many different complementary perspectives on systems, a number of which would provide greater challenges to current thinking.³¹⁸

Civil Service advice incorporates techniques from Soft Systems Thinking (SST) related to power mapping and stakeholder management. Demos' 2022 book promotes SST as a more appropriate method for examining human systems requiring different but potentially equally valid perspectives.³¹⁹

SST places purpose at the centre of its analysis³²⁰ but can risk excluding voices that are less present in current systemic power relationships.³²¹ Incorporating social and environmental perspectives in Systems Thinking requires the use of challenging techniques, as those who need to be heard are likely to be currently excluded, including future generations and people facing disadvantage. Civil servants would need to attempt to ensure that policy communication is free from domination and look at methods of examining systemic disadvantage, such as Critical Systems Heuristics.³²² To avoid systemic exclusion, Critical Systems Thinking proposes that systems be examined by at least two different systems methodologies associated with key perspectives, identified as mechanical, interrelationships, organismic (questions such as resilience), purposeful and social/environmental. The last of these is particularly important where questions of social power are concerned.³²³

Systems Thinking requires open and consistent leadership as well as commitment to strategy to be effective. If interventions are too tightly bound, stop-start, underfunded, fail to iterate, or are siloed in departments, then a civil service doing great systems analysis will not help. Learning from the existing examples of government providing digital leadership is particularly important, but greater devolution and capacity at the top of government may be needed to provide strategic leadership,³²⁴ including building internal expertise³²⁵ and directly shaping digital markets.³²⁶

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Similar points can be made about the use of 'Futures Studies' based on the government's *Futures toolkit*, which is a more speculative but broad analysis of likely changes that could impact government policy choices.³²⁷

Keeping official UK digital chronic risk analysis nearly wholly secret, even when based on Systems Thinking and Futures studies, undermines the value of this work, introduces risks from politically directed exclusion from systems and choices, and restricts the democratic process necessary for managing these risks.

PART III
BEYOND THE UK

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

This is necessarily a whistle-stop tour of some of the interesting work that is taking place outside of the UK, and the benefits that projects are bringing,³²⁸ as well as touching on some of the key economic policy questions.

The number of useful projects listed here should not be taken as meaning that countries are not struggling with abusive relationships with vendors, but rather indicates who, how and why countries are trying to advance the Digital Commons of Open Source as a core part of their Digital Sovereignty strategies.

Digital Sovereignty objectives are being pursued for a mix of strategic and economic reasons. Digital Sovereignty is an active process in the EU and key European countries. Concerns about cloud, AI, and dependency on US tech have aligned with opportunities for revitalising domestic economies. Critically, this is not just 'buy European', but 'promote Open Source'.³²⁹ As OpenForum Europe observes:

... debates about open source in the public sector are no longer primarily about ideology, cost savings or technical preference. They are about economic impact, market structure, Digital Sovereignty and the institutional capacity of public administrations to move from passive consumers to active users of IT.³³⁰

Open Source is frequently seen as the optimal strategy. Studies estimate that investment in Open Source produces four times the economic benefit. National economies would be around 2-3% smaller if Open Source did not exist,³³¹ and Open Source software is found in over 95% of proprietary systems, making up over 70% of these products on average.³³²

Most encouragingly, these projects show that when Digital Sovereignty is reinforced through Open Source, governments can collaborate and share key software development, while simultaneously building their employment and capacity.

Despite the enormous benefits that Open Source and open innovation already deliver, there are weaknesses in the ecosystem that need to be addressed. Specifically, because anyone can use Open Source, there is underinvestment in some critical projects, and sometimes companies that develop successful software find competitors 'freeloading' without contributing to the costs of software development. *Strengthening Open Source* suggests some ways to address this.

LEADING THROUGH STRATEGY, DELIVERY THROUGH DEDICATED INSTITUTIONS

The goals of Digital Sovereignty, especially concerning the ability of the state to control its digital technology, are widely recognised to be best delivered through Open Source technologies and investment. Governments that have succeeded with an Open Source approach have introduced:

- strategies that identify and enforce Open Source as the method or strong preference, including the Netherlands,³³³ France³³⁴ and Germany³³⁵
- institutions that co-ordinate Open Source strategies, such as DINUM (Inter-Ministerial Directorate of Digital Technology) in France, ZenDis in Germany,³³⁶ and OS2 in Denmark. Collectively, these are, sometimes called “Open Source Programme Offices” (OSPOs)³³⁷
- in some cases, multinational governance for Open Source projects such as X-Road and the OpenEHR health record standard and software discussed below.

Until recently, Open Source has not been the normal choice for governments, despite policies in the UK and Europe to prefer it. ‘Institutional capacity’ or the lack of it appears to be critical. Where government strategy supports creating specialised government institutions that manage the process of building Open Source platforms in order to avoid or replace software from incumbent vendors, the strategy can succeed.

Institutions can leverage existing projects and use commercial Open Source vendors and consultants to support government capacity. Because the systems they produce are Open Source, it is easier to build a cohort of engineers inside and outside of government. If vendors or products are unsuitable, they can be replaced.

Government has to ensure it has the internal capacity to manage the development and deployment of its Open Source systems. Meanwhile, the domestic private sector benefits as its Open Source products gain new users paying for high-level support and development contracts.

In the very best examples, multiple governments benefit from the systems that are built, lowering costs globally and enabling technology transfer to the Global South.

BUILDING AI OUTSIDE OF THE US

Europe is also pushing open weight and Open Source AI models. Fully open AI models reference all the data used for training, the technology that produces them, and the 'weights' that make up the AI model. Unlike proprietary models, this makes them attractive wherever accountability and transparency are important. Some EU models have been specifically designed with accountability in mind.

Whether it is the full AI modelling or just the model weights that are made open, users can be given permission to use the model for commercial purposes. Such models speed up the pace of AI adoption by making it cheaper to test different open models, and to deploy and change as technology develops. They reduce vendor lock-in for users, which can be attractive for both commercial and government users. Profitability for AI firms can be sustained through freemium models, customisation, use of APIs or through help deploying models at scale.

In France, preference for Open Source procurement³³⁸ created economic growth including a "9%-18% yearly increase in the number of IT-related startups" as well as Open Source assets that benefit both France and the global economy.³³⁹

Albert API has been built by the French DINUM to ensure that government can swap AI models as it wants.³⁴⁰ DINUM also provide EvalAP, a tool for civil servants to evaluate the performance of different LLMs.³⁴¹

China's strategy for AI also depends on using Open Source, open hardware and open weight models. This was established in 2017, long before export controls on critical hardware were imposed.³⁴² By now, China has produced a substantial ecosystem of high-performing open weight models such as DeepSeek and Qwen, which are popular choices alongside Llama and Mistral for deployments where in-house processing or fine-tuning is desirable.³⁴³ China's AI policy and promotion of Open Source and open weight stretch across its manufacturing sectors, as AI is seen as a general technology, rather than narrowly defined as specifically LLMs and generative AI.³⁴⁴

PURSuing AI GROWTH THROUGH OPEN SOURCE

France has promoted its domestic AI capacity via the Mistral project. While it may appear risky to attempt to compete against closed US or open Chinese

TECH GIANTS AND GIANT SLAYERS

models, Mistral has benefited from the wave of French tech startups, driven by an interventionist French industrial strategy.³⁴⁵ Their open weight models have the advantages of accountability, relative auditability, replaceability and cost, while closed high-performance models are also available. Mistral's annual revenues are now over €340m, and it is set to increase its footprint in 2026. Major investors include the Dutch chip etching tech company ASML.³⁴⁶

Several prominent EU projects such as EuroLLM³⁴⁷ and OpenEuroLLM,³⁴⁸ are designed to be customisable, auditable and more transparent, as well as able to address Europeans' multilingual needs. Financed by the EU with UK involvement, they are expressly intended to stimulate economic activity and promote the use of their open models by making them easier to understand and adapt. Other notable projects include the Swiss project Apertus, also specialising in minority languages, and using open data as the core input, to ensure full transparency.³⁴⁹

CLOUD IN EUROPE

The lack of a cloud industry in Europe is a source of economic pain and worry. The EU cloud market, like the UK's is dominated by Amazon and Microsoft, with Google drawing up as a third operator. European policy analysis has identified vendor lock-in, lack of interoperability, market fragmentation and unfair competition as factors that are holding back European competitors. Unfair cloud licensing was estimated as costing Europe €1bn in 2023.³⁵⁰ Proposed remedies include Open Source, interoperability standards and procurement reform. More controversially, some commentators – and the European Commission itself – are pushing for deregulation, targeting AI and GDPR to remove supposed compliance cost barriers. This “simplification” agenda³⁵¹ has been rejected by trades unions and civil society groups as representing a “rollback of digital rights”.³⁵²

On interoperability, the Eclipse Foundation has proposed an “Open Services Cloud” initiative, which would act as an interoperability layer on different cloud platforms to ensure that customers could move their software from one cloud to another. Based on modelling from mobile switching markets, the Foundation estimates this change would push cloud costs down by 13% over five years and would promote cloud adoption in general.³⁵³ Cloud Infrastructure Services Providers in Europe (CISPE) adds federated cloud technologies as another means for European providers to collaborate.³⁵⁴

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

The European Centre for International Political Economy similarly frames cloud lock-in as a security risk for sovereignty, arguing that “concentration is not the risk, constrained exit is ... switching must be possible, and no firm’s contractual terms should turn continuity [of service through switching] into theory rather than practice”.³⁵⁵

European Digital SMEs are pushing for a ‘Eurostack’ and a preference for buying European in areas of critical technology, including cloud and AI. They argue that procurement criteria should move beyond price to include environmental impacts and other “value-based criteria”.³⁵⁶ CISPE recommends using “functional adequacy” rather than feature parity as a measure of suitability.³⁵⁷ Europe’s Cloud Sovereignty procurement framework already emphasises using multiple criteria designed to assess sovereignty risks rather than purely functional requirements.³⁵⁸

Some emphasise the need for practical steps to overcome the technical gaps in EU cloud provision through Open Source. Berndt Hubert, a Netherlands policy analyst, argues that “significant rework is required to migrate to European alternatives. This is because lots of places have allowed themselves to be locked in to highly proprietary hard to disentangle Cloud services”.³⁵⁹ In his view, the immediate step needed is to build Open Source tools that would fill in missing cloud functionalities, so that the European market can coordinate and compete, and potentially engage in an “Airbus model”.

A further worry in Europe is that the major cloud providers are buying up access to energy infrastructure and thereby locking out other providers from access to energy supply, even when Amazon, Microsoft, or Google do not actually build data centres.³⁶⁰ CISPE also recognises the wider need to ensure that data centres are sustainable,³⁶¹ while France emphasises its decarbonised (nuclear) energy sources as a competitive advantage in its national digital strategy regarding AI.³⁶²

Opinions differ on whether Europe can or should attempt to catch up with the US share of the cloud market as a whole. Confidence has been damaged by the experience of Gaia-X, an EU-financed project to create a federated EU cloud. This project, has not delivered the promised shift in the market, not least because it ended up including the US hyper-scalers.³⁶³ There is, however, widespread recognition that Digital Sovereignty requires governments to lead on building a ‘sovereign’ cloud market to help stimulate EU market share³⁶⁴ through interoperability and other market measures, at the same time reducing price

TECH GIANTS AND GIANT SLAYERS

gouging and artificially inflated market share through service bundling and vendor lock-in. Nevertheless, the practicalities of US dominance mean that there is debate over whether technical-legal protections for cloud can suffice.³⁶⁵

EUROPE AND TECH SECTOR GROWTH

Europe, like the UK, continues to have problems gaining traction for larger tech companies. With cloud, the obvious reason that Amazon, Google, and Microsoft have succeeded is that they have leveraged their existing products to develop capacity and push cloud resales. Access to finance appears to be secondary. AI companies' financiers are placing a bet that their technologies will have general utility and create revenue to match the investment. Arguably, Mistral is the first EU company to try to break through in this way, and its potential advantages in the French and EU markets of language performance, regulatory compliance, and a relatively open approach, which allowing less vendor dependency for its customers, have attracted substantial investment.

The EU is renewing attempts to lower the regulatory barriers for new tech companies to access member states' markets under the "28th regime" proposals,³⁶⁶ and also to "Buy European" in procurement.³⁶⁷ Both have been the subject of long-standing controversy in Europe, so their completion or success is not a foregone conclusion.

OPEN SOURCE PRODUCTIVITY AND DESKTOPS

All governments, departments and institutions need collaboration and office software. It is also core to governments' Digital Sovereignty concerns, as sensitive information is contained in these systems. Combined with Microsoft's rapidly rising prices, it is no surprise that governments, including Germany, France, Denmark and the Netherlands, are making efforts to introduce Open Source,

France's flagship Open Source collaboration product is La Suite, which includes document editing and collaboration, email, chat and video conferencing. Many of these tools are web based, reducing immediate switching costs.³⁶⁸ Most recently, its video conferencing suite Visio began rolling out for 200,000 government employees, replacing Zoom, Google Meet and Microsoft Teams.³⁶⁹

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Tchap, which replaces WhatsApp, Slack and Teams chat in La Suite, is based on Matrix and Element, developed by the UK-French company Element.io and governed by a partnership of tech companies with French government participation.³⁷⁰ It has been adopted as a replacement for Slack or WhatsApp style messaging by NATO³⁷¹ and in the German health system.³⁷²

In Germany, the government's ZenDis³⁷³ funds the desktop software replacement project OpenDesk, based on NextCloud, OpenProject, and other technologies and including the UK-French messaging software Matrix.³⁷⁴ OpenDesk supplies government departments and regional governments. ZenDis works as a consultant to help government institutions to migrate to sovereign Open Source solutions.³⁷⁵ Both work with the private companies that develop the underlying software.

OpenDesk is still in its early stages, but has its first major clients. OpenDesk customers include the Bundeswehr, Robert-Koch-Institute, the Federal Maritime and Hydrographic Agency of Germany, the Federal IT-Cooperation³⁷⁶ and the health service.³⁷⁷ The German Pension Insurance agency and Federal Employment Agency are trialling OpenDesk as part of their back plans for national resilience in a time of crisis – that is, as systems they would be able to use if Microsoft went down.³⁷⁸ OpenDesk components are also used at the Ministry of Digital Affairs and the Federal Chancellery.³⁷⁹ OpenDesk is also used by the International Criminal Court.³⁸⁰

Other municipalities have chosen their own Open Source paths. Munich is gradually moving its services to Open Source, on an 'Open Source first' but case-by-case basis; in France, Lyon is moving to Linux and Open Source collaboration tools.³⁸¹ Meanwhile, in the German state of Schleswig-Holstein, LibreOffice is replacing Microsoft Office and email servers for 30,000 users with the aim of migrating to Linux to replace Windows at a later date.³⁸² In France, between 2008 and 2015, the French Gendarmerie moved 100,000 desktops to Linux Ubuntu and LibreOffice.³⁸³ German procurement policy now mandates the use of the open standard Open Document Formats throughout all levels of government; which should encourage the use of Open Source document editors such as LibreOffice.³⁸⁴

Denmark is assessing how to move away from Microsoft on servers and the desktop³⁸⁵ and the Netherlands is currently evaluating Open Source desktop approaches for national government.³⁸⁶

IDENTITY AND DATA EXCHANGE SYSTEMS

The desire to link government identity systems is common, but controversial. Systems can be either privacy-preserving or create a map of interactions between citizen and state. Whether Open Source or closed and proprietary, ID technologies are frequently controversial because of the privacy implications, and governments have taken a range of approaches to building Open Source government identity systems.

The policy drive to make interactions with government easier has led to several major Open Source initiatives to manage aspects of electronic identity. Open Source systems offer much greater transparency about the risks they are creating, and allow for public scrutiny and debate and also for the creation and adoption of privacy-friendly innovations.

Estonia's Open Source platform, X-Road, allows for information to be passed from one government system to another. It is decentralised, so that information does not need to be held in a single database, and can handle cross-border information requests.³⁸⁷ Other systems handle identity.

X-Road was launched in 2001 and made Open Source in 2016,³⁸⁸ and is now used by Lithuania, Latvia, Iceland, Finland, Brazil, Mexico, Argentina, Cambodia, Colombia, El Salvador, Japan, and Germany.³⁸⁹ The Nordic Institute for Interoperability Solutions manages the project, and offers help to governments wishing to implement the platform.³⁹⁰

Similarly, the EU's eIDAS (electronic identity) and Digital Wallet projects have been produced with Open Source reference implementations which member states can repurpose to provide to their citizens.³⁹¹ X-Road is one option for eIDAS implementations.³⁹²

India's Aadhaar identity system was built with largely interoperable and Open Source components but contains a proprietary core. This led to a collaboration among a number of countries and development funders on the Modular Open Source Identity Platform (MOSIP) project, which replaces the core with Open Source. It is particularly popular in Asia and Africa, and supplies government identity services to over 160 million residents.³⁹³

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Open sourcing the Aadhaar / MOSIP system demonstrates both the benefits and limits to Open Source from a rights perspective. Aadhaar is extremely controversial, as it enables tracking of individuals across systems, and brings other privacy and access issues. Using Open Source may even be a strategy for legitimising its controversial technology, reducing criticisms focusing on untrustworthy vendors.³⁹⁴ Neither Open Source nor open standards can stop governments from making decisions that violate rights, although it does increase the ability of civil society to audit the code or methods and demonstrate the problems.³⁹⁵

The products of MOSIP, X-Road, and the EU's systems have been audited and studied for security, safety and privacy.³⁹⁶ While at times the criticisms may be uncomfortable, the ability to check and suggest improvements – and for governments to explain why not – are an important advantage and can improve trust and reliability overall.

DIGITAL PAYMENTS

Some governments are creating their own digital payment systems to reduce the overheads associated with mobile and card payments. There is potential value in reducing the cost of digital payments for any country. This appears to be the motivation behind the Digital Euro and Digital Pound, for example.³⁹⁷ While 'digital cash' and low friction payments systems can have privacy issues as they log payments and are also less systemically robust than physical cash, it is not surprising that countries are looking to reduce the transaction fees that citizens and businesses pay.

India's Unified Payments Interface, launched in 2016, offers near-zero transaction costs to India's citizens as part of the country's IndiaStack. Brazil launched its own digital payments system, PIX, in 2020. PIX is used by 70% of the population,³⁹⁸ which in 2025 triggered an investigation from the United States Trade Representative into whether PIX unfairly restricts US companies.³⁹⁹ European banks are currently building the 'Wero' European payment system for direct account to account payments through the European Payments Initiative.⁴⁰⁰ This is aimed at reducing customer costs and dependency risks.⁴⁰¹ The UK's banks are also trying to build an alternative card payment system.⁴⁰²

HEALTH AND SOCIAL SYSTEMS

Health systems lend themselves to cross-border co-operation, because many use the same processes. Health has benefited from Open Source and open standards in a number of countries. As noted at *NHS and Palantir, OpenSafely and OpenEHR*, the UK is a significant partner in developing OpenEHR, which is used in the Netherlands, Germany and many other countries. Scandinavian health authorities also use the OpenEHR health record standard, which now enables health providers to use either proprietary or Open Source management tools such as Ethercis. This improves resilience as well as choice, as providers can move systems without losing data.⁴⁰³

District Health Information Software 2, a general platform for health and patient management, has been adopted in over 80 countries in the Global South. The OpenMRS system for patient record management is in use in another 40 countries including Kenya. It has been extended by the Bahmni project to include other common health management functions.⁴⁰⁴ Other notable projects include GNUHealth management software, used by a number of countries and institutions and supported by the GNU Solidario foundation and a regular user conference.⁴⁰⁵ OpenIMIS helps deliver social security, injury and health payments in 13 countries in Africa and Asia; development has been funded by the Swiss and German governments.⁴⁰⁶

EDUCATIONAL TECHNOLOGY

France, Germany, Netherlands, and Denmark are making serious efforts to guarantee the privacy and data protection rights of children and young adults, to build their domestic Edutech sector, and reduce vendor lock-in risks, by deploying Open source systems. Common technologies employed include Moodle, as a general edutech platform, alongside BigBlueButton, for virtual classrooms, and Nextcloud, for document management, collaboration and editing.

The current French education strategy states that, regarding Artificial Intelligence:

Schools must equip students with the tools to understand this technology, to grasp its opportunities as well as its limitations, to

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

develop a critical mindset about it, and, for some—girls and boys alike—to enable them to pursue studies and careers in the field of artificial intelligence ...

While AI represents a challenge and a potential contribution to education, it must nevertheless be used within an ethical and legal framework, in a conscious and reasoned manner, given that the tools currently available are mostly non-sovereign, not free (“libre”), opaque in their operation and training data, and are resource and energy-intensive.⁴⁰⁷

France is developing “sovereign AI to support teachers in preparing lessons and assessing pupils, available from the start of the 2026 school year”.⁴⁰⁸ Sovereign AI in France generally means open weight or fully open AI products, that are deployed on French state controlled infrastructure. This helps alleviate privacy concerns and vendor lock in issue. France’s government has open source national infrastructure, Albert API, discussed at *Pursuing AI growth through Open Source*, which it has developed to allow it to control deployment of such “sovereign AI” systems.

France avoided dependence on US edutech platforms, which has helped it to establish its open source approach. Alexis Kauffmann told a recent panel in Holland that:

One of the key actions is to offer authoring tools to our teacher and tools based on open source software. No Google Classrooms. Not Microsoft Teams. We have chosen Moodle Elea as a learning management system.⁴⁰⁹

The French platform apps.education.fr provides open source infrastructure for French schools and colleges. For example, it provides.⁴¹⁰

- Nextcloud for file storage and sharing, which saw over 100 million files deposited and 330,000 daily users by late 2025.
- PeerTube for video hosting and sharing, hosting over 112,700 videos by the end of 2023
- BigBlueButton for web conferencing and virtual classrooms
- CodiMD (formerly Etherpad) for collaborative text editing

TECH GIANTS AND GIANT SLAYERS

Their next goal is to increase the volume of users to 1.2 million. As the number of users increases, the costs of licensing US products decreases, and the income for French (and British) Open Source tech providers also goes up.

German education is run at state level, so a single picture is harder to discern, but many states have taken the view that use of US (edu)tech is not legally compatible with GDPR. This concern is also driving state level initiatives to move away from US tech giants, exacerbated by general digital sovereignty concerns.

HPI Schul-Cloud illustrates the kind of approach adopted by the German Länder, developed from 2016 and deployed in 2021, and now used in primary and secondary education nationwide. It is a fully open source cloud system for document collaboration, communication and file serving, based on Nextcloud. Roll out was sped up due to the pandemic, and it is now well established.⁴¹¹ It claimed 1 million users in 2021.⁴¹²

Moodle is widely used in the German education sector. By 2020, Moodle was in use by 1.5 million German users.⁴¹³ Moodle is well established as an extensible Open source education platform for course, lesson and content dissemination and submission.⁴¹⁴ It has a strong community of developers across the globe. Moodle is used with Nextcloud and BigBlueButton in Baden-Württemberg, following data protection concerns with Microsoft products.⁴¹⁵

Many education institutions work together in the Netherlands for software development and procurement, through a co-operative called Surf. Since 2025, Surf has been trialling Nextcloud for education use: They explain.⁴¹⁶

In recent years, digital sovereignty has become an increasing theme within and outside our cooperative. Due to the dominance of some large tech companies, our independence and public values are increasingly under pressure. To strengthen our digital sovereignty, we are exploring alternative applications, such as Nextcloud. This is a collaboration environment for word processing, document sharing, email integration and online meetings.

The Netherlands also has an open licensed teaching materials project, to help teachers share lesson materials, plans, etc.⁴¹⁷

Denmark's shift towards Open source Edutech was spurred by a ban on Google Workspace and Chrome books in the province of Elsinor, because of data transfers

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

outside of the EU.⁴¹⁸ While efforts to assuage concerns have been made, the case has caused a shift in thinking across Denmark. A project was set up to provide an Open source alternative to Google Classroom and Microsoft, called OS2 Skole. Danish data ethics commentator Pernille Tranberg says:

Parents and the data authority have particularly protested against the use of Google but it has managed to settle the case by new promises that it will not abuse user data. The agreement between schools and Big Tech is purely based on trust, which to many people is not enough.

Therefore, in the beginning of January 2026, the new school platform was presented to the public. 23 out of 83 municipalities are already backing the project, which can completely disrupt the grip Big Tech has on Danish schools.⁴¹⁹

PROCUREMENT SOFTWARE

Procurement is a core government function. Over 50 countries including the UK have implemented the Open Contracting Data Standard to improve transparency around tenders and bidding throughout the process.⁴²⁰ Based on this standard, Ukraine and Moldova have developed and use the Open Source software Prozorro for bidding processes.⁴²¹ The open standard and Open Source efforts are supported by a charity, the Open Contracting Partnership.

COMMUNITY ENGAGEMENT

Community engagement is a common task for local government. In 2015, at a time of considerable social conflict as a result of austerity, Madrid developed the Open Source platform Consul to handle its consultations and engagement. It amassed 90,000 annual participants and won a UN Public Service Award for its programme of participatory budget making in 2018.⁴²² In 2019, it survived a change of administration.⁴²³ Since then, the software has been adopted in Germany, the Netherlands, Slovenia, Uruguay and Brazil. It is also used by nearly 20 Scottish councils.⁴²⁴ The project is managed by a dedicated, cross-border foundation. A similar system, Decidim from Barcelona, has also seen wide

TECH GIANTS AND GIANT SLAYERS

adoption.⁴²⁵ In Taiwan, the Open Source, wiki-based survey software Polis, which incorporates machine learning, is used as a forum for citizens to share ideas and opinions, reach consensus and help pass legislation.⁴²⁶ It, too, has been used by other governments, including in Singapore and locally in the UK.

INTERNATIONAL COLLABORATION

Collaboration across borders can be seen in many of the projects noted in this section. Countries with similar needs group together to provide open infrastructure projects, such as OpenEHR, Open MRS in health or MOSIP or X-Road for government identity and data transfer.

At the UN level, the Digital Public Goods Alliance, founded in 2019, promotes using and sharing Open Source infrastructure that supports its sustainable development goals.⁴²⁷ Germany joined the alliance in 2021⁴²⁸ and France followed in 2025;⁴²⁹ the UK is not currently a member. The EU also promotes the concept of Digital Public Goods.⁴³⁰ The Open Government Partnership, which the UK joined at its start in 2011, continues to promote transparency and open data.⁴³¹

France is also the first government to sign the Open Source Principles, committing the country to being “Open by default [by] Making Open Source the standard approach for projects”.⁴³²

There is a significant degree of European policy co-ordination. This includes:

- Governmental conferences on Digital Sovereignty
- Open Source sharing between governments
- Promoting interoperable European government technologies such as eIDAS⁴³³
- Tracking Open Source initiatives and policy globally through the Open Source Observatory⁴³⁴
- Investment and policy co-ordination at the EU level
- EU-wide projects to develop open weight, free to use AI LLM models

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

RISC-V: OPEN CHIP DESIGN

Post-COVID chip shortages gave renewed policy focus on the supply of chips. As manufacturers of all kinds require chips for devices, whether they are connected to the Internet or just contain embedded systems, shortages impede industry in general, not just IT suppliers. The stranglehold of just two architectures for chips, from Intel / AMD and ARM, impacts the kinds of chips available as well as supply and pricing. There is an alternative: the open and extensible RISC specification, originally an academic-led project set up in 2010 at Berkeley. A group of academics and commercial users have converged on the current version, RISC-V. ARM chips are also based on RISC design principles, but are not open designs.⁴³⁵

RISC moved its headquarters to Switzerland in 2020 to provide insulation from geopolitical pressures. While some critics have been concerned that open chip technology will inevitably transfer technology to China, the converse risk is that disengagement from the US or others would simply cede leadership to China. Over 4,600 partners from 70 countries, including from the Americas, Europe and China, are involved in RISC.⁴³⁶ Government support comes from the US via DARPA⁴³⁷ and, following the European Chips Act, Europe, which aims to be a leader in RISC-V chip production.⁴³⁸

Chips using RISC-V are increasingly common in low-power devices and for certain AI tasks, and are expected to become commercially practical for desktop use within a decade. About 25% of IoT devices use RISC-V chips.⁴³⁹

RISC-V shows that open innovation can gain ground over purely proprietary development models, even in the expensive and capital-intensive field of chip design.

STRENGTHENING OPEN SOURCE

Open Source development takes place for a variety of reasons. Sometimes, it is led by multinational corporations, such as Google, Amazon or IBM, to deliver key technologies that they jointly rely on. Similar models exist in smaller markets such as web development, for many common tasks and components. This avoids having to licence products, creating dependency. Instead, Open Source allows autonomy and collaboration.

TECH GIANTS AND GIANT SLAYERS

Open Source is commercialised through many different models, including consultancy, maintenance and support services. Software and code are after all just one aspect of delivery. However, because most of the money is made through delivery, there is a risk that companies can 'freeload', leaving development costs to the main developer or foundation, while not contributing in return. With some volunteer-run projects, there can also be a risk that key software components are not maintained, but remain critical to global security needs.

Discussions on how to resolve these problems are ongoing in Europe and in Open Source advocacy. Most recently, the EU Commission ran a consultation on its future Open Digital Ecosystems Strategy.⁴⁴⁰ While the results are not yet published, contributions have been independently analysed by OpenFuture.⁴⁴¹ Potential solutions identified in the consultation include tax incentives for contributing to Open Source and government funds similar to the German Digital Sovereignty Fund to ensure governments invest in the software they depend on. Reforms to procurement could be used to evaluate (or require) that companies that are delivering software prove that they are proportionally contributing to the software they are using, as the Open Source Initiative has suggested.⁴⁴²

Germany's Sovereign Tech Fund directly supports strategically important Open Source projects, including ensuring that code is maintained and kept secure.⁴⁴³ Proposals for the EU to replicate this model⁴⁴⁴ have been supported by Airbus, Dassault and others.⁴⁴⁵

Lastly, care is taken to ensure that Open Source really does mean Open Source. This includes using suitable licences, such as those falling within the definition provided by the Open Source Initiative,⁴⁴⁶ which is frequently cited in policy documents, and even in European laws. Along with this, the supporting Open Standards have to be free to reuse rather than subject to licence fees. For example, care needs to be taken when choosing them to ensure that any patents referenced in standards are expressly freely licenced to all without threat of litigation.⁴⁴⁷

DEMOCRATIC DISCOURSE AND SOCIAL MEDIA REGULATION

ONLINE HARMS IN EUROPE

Questions of online harms, disinformation, misinformation and the amplification of extremist views are as challenging in Europe as in the UK, but the EU's overall

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

approach has overall been more rights based. For example, the Digital Services Act has explicit routes to the courts for content takedown decisions, which the UK's Online Safety Act lacks. Age Verification requirements in Europe are balanced by attempts to ensure the adoption of privacy-protecting technologies, although it is a matter of debate of how to achieve this.

EU discussions on questions of online safety have also generally been more nuanced. For example, many German child protection organisations actively opposed measures such as 'Chat Control', which would have compromised encryption. Europe did not adopt rules demanding encrypted content to be scanned, but has left the door open to member states to try to develop such approaches. These are likely to end up in the Court of Justice if they proceed.

TACKLING PLATFORM POWER THROUGH EU COMPETITION LAW

As in the UK, competition law in the EU has requirements to open up Very Large Online Providers (VLOPs) to competition through interoperability requirements. These are proceeding apace,⁴⁴⁸ creating an impressive number of changes in Apple's iOS App Store and Google's proprietary services for Android such as the Play Store.⁴⁴⁹

Interoperability for messaging platforms such as WhatsApp has been more challenging. WhatsApp has resisted these requirements. For example, Meta says a company providing an interoperable client must ensure that only European customers can benefit from and communicate through an interoperable client.⁴⁵⁰ This requires a very high level of tracking of customers which many companies do not wish to engage in. It also undermines the point of communicating with an international platform.

ADDRESSING ONLINE HARMS THROUGH COMPETITION LAW

Protecting democratic discourse is a significant theme in European Digital Sovereignty policies, some of which have explicitly mentioned developing alternative European social media. Support for Mastodon has come from EU⁴⁵¹ and German experiments⁴⁵² in running their own Mastodon servers to broadcast official content and by providing financial support for Mastodon's development from the German Sovereign Tech Fund.⁴⁵³

Discussions have recognised the benefits of decentralised social media for online safety. The German organisation Hate Aid argues that the social media models

TECH GIANTS AND GIANT SLAYERS

found on Mastodon produce safer online environments by taking a user-centred and structural approach to safety.⁴⁵⁴ Similarly, the Polish NGO Panoptykon proposes to tackle the business model of recommendation systems by viewing giving users control as a consumer safety intervention, and wants to see legislation requiring these to be opened up.⁴⁵⁵

However, despite demands from civil society, the Digital Markets Act did not include interoperability for social media so that users can move more easily to safer, more user-focused platforms (see *Online political distortion, Social media policy*).⁴⁵⁶ This was a major oversight, but future reviews may reopen the question.

There has been a legal trend towards viewing competition law as an instrument for addressing social and environmental harms relating to a market actor's dominance. This reflects a general shift away from the standard of 'consumer welfare' which had dominated competition policy until fairly recently. A consumer welfare analysis of Facebook, for example, would see no harm, as the service is provided for free.

German competition law now allows abuses that originate from a dominant position, but are not competition law abuses, to be targeted for remedies, particularly with respect to data protection. Facebook and Meta have been instructed that they cannot combine different datasets without user consent, including those held by other services it owns, like Instagram, and third party websites.⁴⁵⁷ This ruling is based on Section 19a of the German Competition Act, which allows the Bundeskartellamt to restrict various practices when a company is dominant.⁴⁵⁸ Overall, German and European competition law is moving back towards a more interventionist model of shaping responsible behaviour and competition, known in Germany as the 'Ordoliberal' approach.⁴⁵⁹

The Netherlands incorporates consumer protection into competition enforcement. The Dutch Consumer and Markets Authority's priorities in 2025 included: "Fair access to online markets for people and businesses"; "Safe and accessible online environments: protecting online users"; and measures aimed at "Sharing data securely and reliably for innovation".

The Dutch approach to consumer and market enforcement is echoed in research activities which aim to extend the understanding of competition harms through a 'capability' approach. Consumers have rights to property and to contract ('market-forming' capabilities), consumptive capabilities for health and education. Third-

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

party capabilities can include effects on future generations, animal welfare, and so on. Being certainly more radical than the current competition paradigm, this approach suggests interesting ways forward for restraining the power and impact of tech giants.⁴⁶⁰

PART IV
RECOMMENDATIONS FOR A DIGITAL
SOVEREIGNTY STRATEGY

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

We can use the UK's and its partners' past successes and failures to devise criteria for a successful Digital Sovereignty strategy.

Given trade-offs, such as the costs of changing from existing proprietary software, a shift in mentality, incentives and organisation are needed. These should include a preference for procuring Open Source solutions that deliver long term autonomy; investment in the technologies; a build up of UK Open Source technical capacity in the private sector; and the creation of specific institutions⁴⁶¹ within government to handle cross-cutting areas of tech.⁴⁶²

An outward-looking Digital Sovereignty strategy would build on the UK's role in shaping global rules, rather than retreating into technological autarky. By prioritising open standards, interoperability and Open Source capacity, the UK can secure long-term strategic autonomy while reinforcing global digital trade, technology transfer, and equitable, sustainable development. In this model, sovereignty is developed and exercised through collaboration and influence over technical and governance architectures, not through isolation.

WHERE TO START

Restoring Digital Sovereignty will be a process not an event. It starts with recognising and being transparent about the risks outlined in *Part I The Digital Sovereignty challenge*, then realigning the UK's strategy deficits shown in *Part II Current UK policy position*, by learning from the good experience we outlined in the same section, and from the global and European efforts outlined in *Part III Beyond the UK*.

Digital technologies of particular concern include desktop and collaboration software, cloud systems, and the AI economy. Defence software is also an area of concern. Health is a risk and an opportunity, as is local government.

Desktop and collaboration software should be prioritised for attention because both can be easily disrupted, and the Digital Sovereignty cost is currently significant. Because Microsoft is a de facto monopoly supplier, significant financial gains can be made simply by opening up the UK to Open Source alternatives. Such systems can also be deployed as a 'plan B', as some German departments have done.

TECH GIANTS AND GIANT SLAYERS

Cloud systems are harder to shift, and lock-in is significant, so a concerted effort is needed to align with the aims of Digital Sovereignty. Enforcing laws against competition harms would reduce the price pain for the whole UK economy.

With AI, given the investment costs, ensuring strategic autonomy involves working with Europe, for example to ensure continued development of fully open AI systems. This is already taking place in research, but is far less evident in procurement and industrial policy.

REGULATORY AND ECONOMIC ALIGNMENT WITH EUROPE, OPEN INNOVATION WITH THE US

Economic realignment and growing the UK tech sector to reinforce its own momentum may need co-operation and greater alignment with European partners. Regulators will need to act independently, and government will need to encourage them to do their job and take regulatory action rather than shy away from it. These also imply closer relationships with Europe, rather than the current strategy of over-reliance on US tech investment with extractive risks. The strategy choice would appear to be between ever-greater dependence and risk through the current form of close ties to the US, and a more balanced interdependence bolstered by closer relations with the EU, and developing more equitable and de-risked open innovation-based trade with both the EU and US. Some of the products from IBM and RedHat offer the kind of Open Innovation trade model that would work for the UK and US, for example.

GIANTS AND GIANT SLAYERS

Open Source is critical to the Digital Sovereignty agenda set out in France, Germany, the Netherlands, Denmark and elsewhere. Careful attention is needed to ensure that the Open Source sector is supported and developed in the UK.

Open Source dynamics can favour SMEs, because any business with the right skills can enter an Open Source market. As noted in the introduction, most tech giants seek to corner the market and profit from monopoly.

Many global giants also contribute to Open Source. IBM supplies managed Open Source products, including through its Red Hat subsidiary, an established Linux

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

vendor. Where Open Source excels is levelling the playing field, so that IBM and Red Hat compete with other Linux suppliers on convenience, security and reliability, rather than using the pain of change to prevent exit.

Open Source SMEs in the UK include: Canonical,⁴⁶³ which supplies Ubuntu Linux; Collabora,⁴⁶⁴ which supplies the Collabora online editor; RaspberryPi the educational tech developer and manufacturer;⁴⁶⁵ and Element, a French-UK company that supplies encrypted chat products to the Open Source world, European governments and NATO.⁴⁶⁶

Companies in the Open Source sector rely on reputation and trust, supplying expertise and support. It is therefore not as necessary for an Open Source provider to seek to demolish and swallow all competition. Because a solution may not fit all needs forever, it may have to innovate or risk decline. Companies that breach trust, change licenses or change their ethics tend to lose other Open Source customers.

Government could do much more to support Open Source through contracting and prioritising Open Source. Similar to those of the EU's cloud procurement practices (*Cloud in Europe*),⁴⁶⁷ procurement criteria could include: assessing interoperability; reusability; absence of vendor lock-in; Digital Sovereignty; and total cost of ownership. Procurement can presume or require Open Source, and ensure that Open Source is assessed so it can be used where viable or where the Government judges that bespoke software is needed. Procurement could consider the total economic value of an investment, rather than just the cost to government; Open Source is likely to be better value when the value of releasing code to the economy is taken into account (see *Introduction*).

Government could also work with business schools and computer science courses to ensure they cover Open Source development and business models, so that these approaches are better understood and promoted as a viable option.

DIGITAL LEADERSHIP

As the discussions of *Government Digital Service* and *Wales and Scotland*, and other national and international governance models detailed in *Leading through strategy, delivery through dedicated institutions* and *International collaboration* have showed, it is necessary to build internal expertise and leadership to deliver

TECH GIANTS AND GIANT SLAYERS

Open Source, sovereign technologies. Doing so can reverse the long-term trend of outsourcing all aspects of IT delivery and dependency on consultants, a strategy which, as outlined in *UK spending on digital technologies*, has proved repeatedly disastrous for the UK.

Institutional leadership models are common in the Open Source world. Many Open Source software projects are split between a 'foundation' controlled by the main suppliers or users, which develops the software itself, and commercial actors who supply it. This is the model chosen by many of the government-led Open Source products such as X-Road. In some cases, institutional leadership for major IT systems may be through a statutory body set up for the purpose; this model can be especially important when there are questions of social accountability, or express needs to limit the a system's purposes.⁴⁶⁸

PROTECTING DEMOCRACY

Countering the market power of social media giants so as to diversify the social media and online advertising markets is critical for democratic discourse. As outlined in *Social media policy*, and *Addressing online harms through competition law*, interventions to open up social media and enabling user switching and third-party control of prioritisation algorithms and moderation engines would help align social media business models with users' needs for a pluralistic and safe information environment. Government can also take simple steps to support the alternative, open models, rather than simply propping up corrosive platforms with content and ad spending.

A ROADMAP FOR DIGITAL SOVEREIGNTY

1. Reset UK digital policy

1.1 Set Digital Sovereignty goals as key for UK national strategy and risk management

(Part II Current UK policy position)

1.2 Release a full version of the already-completed analysis of the “chronic” risks from Global tech, AI reliance, E2EE and tech concentration

(Part II Current UK policy position, Systems thinking and UK Digital Sovereignty)

1.3 Modify the Industrial Strategy sectoral plan for IT to:

1.3.1 Promote domestic expertise and industry

(Economic dependency and extraction, Building AI outside of the US, Europe and tech sector growth)

1.3.2 Promote Tech growth based on Open Innovation including Open Source and open hardware such as the RISC-V chip design

(Vendor lock-in, RISC-V: open chip design, Strengthening Open Source)

1.3.3 Provide a UK Sovereign Tech fund to ensure the Open Source technologies the UK depends on or needs are both secure and developed

(Strengthening Open Source)

1.3.4 Create cross-border, especially European, collaboration on AI and cloud technologies and standards

(Cloud and AI lock-in, AI procurement, Building AI outside of the US, Cloud in Europe)

1.3.5 Promote strong competition and data protection enforcement to ensure market incentives align with UK social values and users’ needs

(Competition policy, Data protection)

1.3.6 Task the CMA with driving value in cloud and AI through strong competition interventions

(Cloud and AI lock-in, Competition policy, UK and Cloud suppliers)

1.3.7 Extend the harms competition law can address from pure market harms to consumer and third-party harms resulting from market domination

(Tackling platform power through EU competition law, Addressing online harms through competition law)

TECH GIANTS AND GIANT SLAYERS

1.4 Modify the Modern Digital Government plan to

1.4.1 Set Digital Sovereignty at the centre of its goals

(Part II Current UK policy position, The Growth Agenda)

1.4.2 Place Open Source and Open Standards as front and centre of the strategy

(The Digital Commons: Open technologies; Vendor lock-in; Strengthening Open Source)

1.4.3 Deliver sovereign, open weight AI and modular, replaceable AI to avoid new lock-in

(AI procurement, Building AI outside of the US)

1.4.4 Review relationships with vendors that do not deliver on Digital Sovereignty, and plan exits based on their risks and benefits

(Where to start)

1.4.5 Explain and develop a new model of IT leadership across government as set out below

(Digital leadership)

1.4.6 Deliver changes to procurement and international collaboration as set out below

1.5 Prevent the sale of key companies

1.5.1 Prevent foreign acquisitions of any size within strategic sectors where this would create a national security risk

(Mergers and acquisitions)

1.5.2 De-risk critical projects by ensuring they are led by foundations without beneficial ownership

(Health and social systems, Strengthening Open Source)

1.5.3 Where software systems form a natural monopoly, prefer companies without beneficial ownership.

(Strengthening Open Source)

1.6 Drive competition and effective regulation

1.6.1 Bar the 'revolving door' in and out of UK regulators at the highest levels.

(Lobbying and astroturfing, Competition policy, Data protection)

1.6.2 Instruct regulators to act independently to enforce the law, and disavow attempts to 'steer' their activities

(Competition policy, Mergers and acquisitions, Data protection)

1.7 Ensure better policy development by:

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

- 1.7.1 Inviting comment on the government's full analysis of the tech-related chronic risks identified in the 2025 National Risk Register and Chronic Risks document, to ensure that the official view of their policy systems, interactions and dynamics, including what is included and excluded from consideration, is subject to rigorous external testing and drives public debate
(Systems thinking and UK Digital Sovereignty)

2 Build digital leadership

2.1 Devolve IT leadership

- 2.1.1 Adopt Estonia, Germany, France and India's model of technology leadership and open systems in IT development for core UK systems

(Identity and data exchange systems, Health and social systems, International collaboration)

- 2.1.2 Support initiatives such as the National Police Digital Services to take on more sectoral support

(Digital sovereignty beyond Whitehall, Local government, Wales and Scotland)

- 2.1.3 Identify areas where new foundations can lead core aspects of central or local government capacity

(Digital sovereignty beyond Whitehall, Local government, Wales and Scotland)

3 Deliver 'Public Code for Public Money'

- 3.1 Presume Open Source and require an assessment of available Open Source components in procurement

(Strengthening Open Source)

- 3.2 Ensure procurement templates are designed with Open Source in mind.

(Strengthening Open Source)

- 3.3 Consider the total economic value of the product, by factoring in the likely value to third parties (individuals, organisations and governments) of any code released to them

(Strengthening Open Source)

- 3.4 Ensure Government owns the source code that it commissions others to write, thereby allowing it to be opened and improved by other users and vendors

(Vendor lock-in)

- 3.5 Where UK government sectors are currently monolithic or served by dominant partners, for example in desktop software or enterprise

TECH GIANTS AND GIANT SLAYERS

databases, develop alternatives to ensure competition and choice
(*Vendor lock-in; Open Source productivity and desktops*)

4 Drive Open Standards, Open Source and interoperability

4.1 Prohibit tenders from requiring specific proprietary solutions or proprietary software or standards requiring charges for patent usage.

(*Giants and Giant slayers, Strengthening Open Source*)

4.2 Consider interoperability, reusability, vendor lock-in, Digital Sovereignty, and total cost of ownership as procurement criteria.

(*Giants and Giant slayers, Strengthening Open Source*)

4.3 Produce guidance on avoiding vendor lock-in with AI products

(*AI procurement, Building AI outside of the US*)

4.4 Ensure the private sector invests in the Open Source it uses by adding procurement criteria that expect the supplier to contribute code and financial resources to Open Source components they depend on.

(*Giants and Giant slayers*)

4.5 Help the private sector develop Open Source in businesses

4.5.1 Make Open Source contributions tax deductible

(*Giants and Giant slayers, Strengthening Open Source*)

4.5.2 Work with business schools and computer science courses to ensure they cover Open Source development and business models

(*Strengthening Open Source*)

5 Ensure international collaboration

5.1 Ensure that a range of companies provide Open Source technologies from all parts of the democratic world, while ensuring technology, expertise, and local options for support is developed in the UK

(*International collaboration*)

5.2 Join the UN Digital Public Goods Alliance

(*International collaboration*)

5.3 Lead and contribute to Digital Public Goods through development funding

(*International collaboration*)

5.4 Provide support for Open Source through international development agencies

(*Health and social systems, International collaboration*)

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

5.5 Assess where the UK could join or lead international Open Source efforts for government, similar to X-Road

(Identity and data exchange systems, Health and social systems, Educational technology, International collaboration)

5.6 Join European efforts on AI development and ensure that benefits from our collaborations are successfully commercialised

(Building AI outside of the US, Pursuing AI growth through Open Source)

5.7 Ensure regulatory co-operation and alignment with Europe.

(European and international collaboration, Regulatory and economic alignment with Europe, open innovation with the US)

5.8 Deepen Open Innovation-based trade with the US

(Regulatory and economic alignment with Europe, open innovation with the US)

6 Drive open social media to reduce Online Harms

6.1 Ensure government supports social media based on interoperable, open standards as well as closed platforms.

(Online political distortion, Social media policy)

6.2 Require the largest social media companies to open up communications with their users from other platforms, and to allow competitors to access and change their recommendation systems through legislation or competition regulation.

(Social media policy, Addressing online harms through competition law)

6.3 Change competition law to allow enforcement to prevent social and environmental harms flowing from market dominance

(Addressing online harms through competition law)

APPENDIX I

UK TECH COMPANIES SOLD OVERSEAS

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Tech company	Year	Sale value	Details
ARM sale to SoftBank (Japan)	2016	£24.3bn	Sale made in wake of Brexit vote and low value of the pound. Was not blocked but some guarantees put in place. ⁴⁶⁹ Sale criticised by the Research and Development Society as losing UK control of a strategic asset, the UK's most important tech company. ⁴⁷⁰
ARM sale to NVIDIA (blocked); ⁴⁷¹ listed on US stock exchange ⁴⁷²	2022	\$40bn	Blocked by US Federal Trade Commission, then listed on US stock exchange.
Autonomy sale to HP (US) ⁴⁷³	2011	£7.4bn	Specialised in big data analytics, disputes over sale value ensued.
Telecity to Equinix (US) ⁴⁷⁴	2015-16	£2.45bn	Blocked a merger with a Netherlands company that could have created a European data centre company with global scale.
Imagination Tech to Canyon Bridge Capital Partners (China) ⁴⁷⁵	2017	£550m	UK chip maker, supplying Graphics Processing Units (GPUs) to Apple for phones.
DeepMind to Google (US) ⁴⁷⁶	2014	£240m	Developed learning algorithms using Machine Learning and systems neuroscience.
SwiftKey to Microsoft (US) ⁴⁷⁷	2016	£250m	Text prediction software used in smartphones.
TTP Communications to Motorola (US) ⁴⁷⁸	2006	£103m	3G technology for mobile handsets. Motorola failed to integrate the company and their Cambridge facilities shut in 2008.

TECH GIANTS AND GIANT SLAYERS

Magic Pony to Twitter (US) ⁴⁷⁹	2016	£102m	Machine learning for image processing.
-------------------------------------------	------	-------	----------------------------------------

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

APPENDIX II

SECURITY RISKS, OPEN VS CLOSED TECH

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Proprietary technology	Open technology
Security problems and fixes must be spotted and fixed by the vendor.	Security problems can be fixed by any third party with the right skills and knowledge.
Code cannot be audited or is expensive to audit.	Code is auditable.
Terms of service, ownership and products' future are subject to vendor choice.	Products can be adapted by any third party. Terms of service can be negotiated with multiple vendors to ensure government priorities are met.
If foreign owned, they may be subject to extra territorial powers of access such as the US FISA and CLOUD Acts, or can be the subject of sanction regimes, etc.	Vendors can be changed if or when this is viewed as a significant risk.
When very dominant, they can form a single point of failure.	Software can be supplied from multiple sources, much easier to avoid risks of single points of failure.
If UK owned, they may be sold to a foreign company, unless government is prepared to intervene.	If a UK vendor is sold to a foreign company, the vendor can be replaced while using the same software
Like-for-like substitution may not exist.	Like-for-like substitution of vendors is always possible. Software may be changed or adapted to meet new needs without permission of the original vendor.

APPENDIX III

SOVEREIGNTY RISK MANAGEMENT

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Risk to sovereignty	Partial mitigations	Effective mitigations	Best practice examples
Security of systems			
External access to UK data in the cloud	'Sovereign Cloud' Domestic owned infrastructure	Domestic located and owned cloud technology based on Open Source technology	
External access to or use of physical equipment, including through embedded software	Testing of equipment Code audits	Open hardware design eg RISC-V chips	RISC-V chip design, support from EU and Germany. Ending Huawei contracts
Ending software support through sanctions etc	'Sovereign Cloud' Exit strategies Ready to go second software systems	Open Source systems	La Suite, OpenDesk deployment at ICC
Dependence on non-UK vendors	Switchable systems (move from vendor to vendor)	Open Source systems with established UK market	Government web estate, IBM / RedHat cloud
Economic risks			
Economic dependence and extraction from US-based AI industry	Switchable systems (move from vendor to vendor)	Develop open AI technology Use of open weight models Grow UK-EU partnerships	Server tech including: VLLM Huggingface NVIDIA Triton server Models incl: Mistral, LLaMA, Falcon, BLOOM Projects incl EuroLLM (EU-led partnership including British)

TECH GIANTS AND GIANT SLAYERS

			universities)
Unaccountable proprietary AI systems	Ask vendors to develop accountability tools	Develop open technology aimed at end to end transparency	OpenEuroLLM EuroLLM Open Model Initiative BLOOM StarCoder
Value for money in government IT spending	Switchable systems (interoperability and open standards) Internal expertise and management	Open Source systems Development with other governments of key infrastructure needs.	GDS ZenDis X-Road and Nordic Institute for Interoperability Solutions
Economic growth from government IT spending	Buy from UK businesses especially SMEs	Buy UK from partners developing Open Source systems (four times multiplier)	
Economic extraction from US takeovers	Examine takeovers for risks Impose takeover conditions	Block strategic sales of key tech businesses Ensure access to EU market Develop financing at scale with EU for tech sector	French and German approaches to acquisitions
Social and political risks			
Distortion of online information ecology	Regulate companies for content but not their business model (Online Safety Act)	Competition policy to orient companies towards the needs of users not advertisers User empowerment over algorithms and content	CMA (UK) and DMA (EU) powers BlueSky and Mastodon / ActivityPub services EU and DE funding for Mastodon / ActivityPub

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

		prioritisation UK / EU operators within switchable social media networks	
Vendor-led policy making	Regulation of technologies	In-house development of capabilities, with other governments where possible	GDS, ZenDis, DINUM, etc
Limits to rights through trade treaties	Transparency Parliamentary scrutiny and votes for agreements Maintain strategic autonomy so choices are better	Enforceable rights basis for treaty agreements	EU trade treaty process (requires Parliament to vote on trade treaties); treaties subject to EU charter of fundamental rights.

APPENDIX IV

UK TECH STRATEGIC SUPPLIERS

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

Strategic supplier ⁴⁸⁰	Famous for	Domiciled, Direct revenue 2024-5 ⁴⁸¹
Accenture, IT and digital consulting	Could not be removed from National Insurance systems by HMRC despite attempts to end the Aspire contract in 2016-17. New contracts awarded in 2025. Removing them would place key systems “at risk”. ⁴⁸²	Dublin £403m
Atos, Communication s, cloud computing, and cyber security	AWPP / NEST awarded Atos contract to move away from Tata technologies, cancelled and returned to Tata in 2023 after two years. ⁴⁸³ Major contracts awarded in 2021-2. ⁴⁸⁴ Company while facing difficulties awarded further years of contracts worth £474m by government bank, National Savings and Investments. ⁴⁸⁵	France £660m
AWS (Amazon Web Services) Cloud computing services	Charging for data exit fees, Competition and Markets Authority wants to designate it as having control of the market (Strategic Market Operator). ⁴⁸⁶ Government concerns that the UK may no longer be able to negotiate with AWS and MS Cloud. ⁴⁸⁷	US £300m
Capita Business process outsourcing and professional services	So bad but so embedded that it could not be removed, ⁴⁸⁸ given new civil service pension scheme contracts in 2025, after 11-year gap. ⁴⁸⁹ Delivery problems emerge, including long processing backlogs. ⁴⁹⁰	London £684m

TECH GIANTS AND GIANT SLAYERS

<p>Capgemini Consulting, technology, and outsourcing services</p>	<p>So bad the Conservatives attempted to sack it at HMRC in 2016-17 but couldn't as too embedded; contract of £107m awarded again without competition in 2025.⁴⁹¹</p>	<p>France £885m</p>
<p>Computacenter IT infrastructure services</p>	<p>Supplied substandard laptops infested with malware, at double the market price. Key financial information omitted from published contracts.⁴⁹² No open tender for the project.⁴⁹³</p>	<p>Hatfield UK £448m</p>
<p>CGI IT and business consulting services</p>	<p>Merged with Computer Sciences Corporation (CSC), a key contractor in the NHS National Programme for IT (NPFIT), "one of the worst and most expensive contracting fiascos in the history of the public sector". Contracted at HMRC in 2025 for Enterprise Integration Services,⁴⁹⁴ and the Home Office in 2022.⁴⁹⁵</p>	<p>Canada £358m</p>
<p>DXC Technology IT services and consulting</p>	<p>Supplier of MoD personnel system transferred to Microsoft Azure cloud, worth £900m, beset by failings and delays in 2017.⁴⁹⁶ DWP cancelled two hosting and desktop contracts in 2017, systems moved to cloud.⁴⁹⁷ Oracle contract negotiated by DXC for Sussex County Council cost double the normal price in 2025.⁴⁹⁸</p>	<p>US £101m</p>

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

<p>Fujitsu IT equipment and services</p>	<p>Post Office Horizon scandal and other failures led to Fujitsu committing to pause new contracts in 2024, but a new £220m deal was signed for HMRC data systems months later, as the only contractor capable of maintaining the system.⁴⁹⁹ Replacement likely to be a hyperscaler.⁵⁰⁰ A total of £510m worth of contracts was awarded to Fujitsu after the 'pause' by July 2025, many without competitive tendering.⁵⁰¹</p>	<p>Japan £453m</p>
<p>IBM Hardware, software, and consulting</p>	<p>Post Office paid £16m to IBM for cancelled project to replace Fujitsu for Horizon.⁵⁰² Emergency Services Network (ESN) suffered persistent delays and was the subject of Parliamentary inquiries.⁵⁰³ Delivered poor components including a mobile app with limited functionality in the National Savings & Investments (NS&I) transformation.⁵⁰⁴</p>	<p>US £426m</p>
<p>Microsoft Software, services, and devices</p>	<p>Overcharging at non-MS cloud services through "Bring your own licence". Contracts of £700m at the NHS.⁵⁰⁵ Criticism over costs rising to £1.9bn a year for cross-government contracts.⁵⁰⁶ Fees are rising fast⁵⁰⁷ as Microsoft attempts to recoup AI and cloud costs with little market resistance.⁵⁰⁸</p>	<p>Redmond US £160m</p>

TECH GIANTS AND GIANT SLAYERS

<p>Oracle Database software and technology, cloud systems</p>	<p>Multiple issues and cost overruns from £20m to up to £170m moving to Oracle from SAP, at Birmingham Council,⁵⁰⁹ contributing to its declaration of bankruptcy,⁵¹⁰ and at West Sussex with cost escalations of 15 times the initial estimate.⁵¹¹ Continued awards by central government.⁵¹²</p>	<p>Santa Clara US £358m</p>
<p>Sopra Steria IT services and consulting</p>	<p>EVisas at the Home Office⁵¹³ and passport scanning (as delivery agent as well as software company).⁵¹⁴ Affected by the Ryuk ransomware attack in 2020.⁵¹⁵ Contributed to security breaches at MoJ prisoner rehabilitation services as a subcontractor.⁵¹⁶</p>	<p>France £309m</p>

THE CASE FOR DIGITAL SOVEREIGNTY AND THE DIGITAL COMMONS

REFERENCES

- 1 Blind, K., & Schubert, T. (2024). "[Estimating the GDP effect of Open Source Software and its complementarities with R&D and patents: evidence and policy implications.](#)" *The Journal of Technology Transfer*, 49, 466-491.
- 2 Synopsys Cybersecurity Research Center (CyRC). (2023). "[2023 Open Source Security and Risk Analysis Report.](#)" Synopsys, Inc.
- 3 Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Patsch, S., & Schubert, T. (2021). "[The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy. Final Study Report.](#)" European Commission, Directorate-General for Communications Networks, Content and Technology. Publications Office of the European Union.
- 4 The Linux Foundation. (February 2026). [ROI for Open Source Software Contribution: Insight from the Open Source ROI Survey and Economic Model.](#) The Linux Foundation.
- 5 Examples include La Suite <https://lasuite.numerique.gouv.fr/en>
- 6 Nagle, Frank (2019) "[Government Technology Policy, Social Value, and National Competitiveness](#)". Harvard Business School Strategy Unit Working Paper No. 19-103,
- 7 OpenUK. (July 2023). [Open Source contributes £13.59 billion GVA to UK economy, finds OpenUK.](#) Press Release. OpenUK.
- 8 Hoffmann, M, Nagle, F and Zhou, Y, (2024) "[The Value of Open Source Software](#)" Harvard Business School Strategy Unit Working Paper No. 24-038.
- 9 Blind, K.; Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Patsch, S., Schubert, T. (2021). [The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy. Final Study Report.](#) Brussels.
- 10 Sayers, O. (2024) "[Microsoft's ICC email block reignites European data sovereignty concerns](#)", *Computer Weekly*
- 11 Undinmwén, E. (2025) "[Denmark wants to replace Windows and Office with Linux and LibreOffice as it seeks to embrace digital sovereignty](#)". *Techradar*. Digital Hub Denmark (2025) "[Decoding: Europe can't regulate its way to digital sovereignty. It must build it.](#)"
- 12 Hüscher, P., & Williams-Dunning, S. (September 2025). "[A Big, Beautiful US Investment Boost for the UK Tech Sector?](#)" *Royal United Services Institute Commentary*.
- 13 See *Digital payments* below.
- 14 Bria, F, Bautista, J. (2025) "[The Authoritarian Stack](#)".
- 15 Marzouk, A. (2025). "[Death of Twitter and the rise of X: The birth of the digital authoritarian context](#)". *Dialogues on Digital Society*, 1(3), 338-342. Gauthier, G., Hodler, R., Widmer, P. et al. (2026) "[The political effects of X's feed algorithm](#)". *Nature* (2026).
- 16 Hancock, J. (June 2025). "[Tech Oligarchy Imperils Democratic Information Flows.](#)" *Tech Policy Press*.
- 17 Shaleen Khanal, Hongzhou Zhang, Araz Taelhagh, "[Why and how is the power of Big Tech increasing in the policy process? The case of generative AI](#)", *Policy and Society*, Volume 44, Issue 1, January 2025, Pages 52–69
- 18 Portmanteu of 'satisfy' and 'suffice'; Artinger, Florian M.; Gigerenzer, Gerd; Jacobs, Perke (2022). "[Satisficing: Integrating Two Traditions](#)". *Journal of Economic Literature*. 60 (2): 598–635.
- 19 See 'UK spending on digital technologies' below, and National Audit Office (2024) "[Government's approach to technology suppliers: addressing the challenges](#)" Gov.uk.
- 20 NAO 2024; also Freedman, Sam (2024) "Failed State" Pan Macmillian. pp. 50-54.
- 21 Blind, K., & Schubert, T. (2024). "[Estimating the GDP effect of Open Source Software and its complementarities with R&D and patents: evidence and policy implications.](#)" *The Journal of Technology Transfer*, 49, 466-491.
- 22 Synopsys Cybersecurity Research Center (CyRC). (2023). "[2023 Open Source Security and Risk Analysis Report.](#)" Synopsys, Inc.
- 23 Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Patsch, S., & Schubert, T. (2021). "[The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy. Final Study Report.](#)" European Commission, Directorate-General for Communications Networks, Content and Technology. Publications Office of the European Union.
- 24 Hoffmann, M., Nagle, F., & Zhou, Y. (2024). "[The Value of Open Source Software](#)". Harvard Business School Working Paper 24-038. Harvard Business School.
- 25 Nagle, F. (2019). "[Government Technology Policy, Social Value, and National Competitiveness](#)". Harvard Business School Strategy Unit Working Paper No. 19-103.
- 26 Benhamou, Y, Bernard, F and Durand, C. "Digital Sovereignty in Switzerland : the laboratory of federalism". In [Risiko & Recht](#), 2023, 1 p. 65–101.
- 27 Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). "[Digital sovereignty — Rhetoric and reality](#)". *Journal of European Public Policy*, 31(8), 2099–2120.
- 28 DINUM (2023) "[Le numérique au sein de l'État](#)". Gouv.fr
- 29 Falkner, Heidebrecht and Seidl 2024.
- 30 Federal Government of Germany (Scholz Government). (August 2022). "[Digital Strategy — Creating Digital Values Together](#)".

- 31 Presse- und Informationsamt der Bundesregierung. (November 2025). "[Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe](#)".
- 32 Ruiz, Javier (2015) "[Collect it all: GCHQ and Mass surveillance](#)". Open Rights Group. See "1.3 Digital Communications" on the Muscular programme of access to Google cabling, and "5.5 Prism and the UK" on US access to back end systems. The efforts made to collect from Google's private cabling, we possible as they were not using encryption; and the Prism system to interrogate US holders of personal information such as Facebook was based on FISA powers. US powers are outlined below, "*Legal risks*".
- 33 Couture, S., & Toupin, S. (2019). "[What does the notion of "sovereignty" mean when referring to the digital?](#)" *New Media & Society*, 21(10), 2305-2322.
- 34 Op cit.
- 35 Hauser, H. (2021). "[Technology, Sovereignty and Realpolitik](#)". In: Wang, H., Michie, A. (eds) *Consensus or Conflict?. China and Globalization*. Springer, Singapore.
- 36 Komaitis, K (October 2025) "[Interoperable Sovereignty: The Democratic Alternative to Digital Authoritarianism](#)". *Komaitis.org*.
- 37 Rikap C, Durand, C, Paraná, E, Gerbaudo, P and Marx, P. (2024). "[Reclaiming digital sovereignty: A roadmap to build a digital stack for people and the planet.](#)"
- 38 Kapur, A. (2024). "[From Digital Sovereignty to Digital Agency](#)". *New America*.
- 39 Barasa, Hilda; Tay, Peichin; McBride, Keegan; Iosad, Alexander; Mökander, Jakob (January 2026). "[Sovereignty in the Age of AI: Strategic Choices, Structural Dependencies and the Long Game Ahead](#)". Tony Blair Institute for Global Change. p8
- 40 See for example: Atkinson, R. D. (2026). [The Case for Policy Transformation to Avoid Losing the Techno-Economic-Trade War With China](#). Information Technology and Innovation Foundation. For the Biden administration, see The White House. (2022). [National Security Strategy](#). For a view from Congress, see: US-China Economic and Security Review Commission. (2024). "[Chapter 3: U.S.-China Competition in Emerging Technologies](#)". In *2024 Annual Report to Congress*.
- 41 EU Commission (October 2025) "[Cloud Sovereignty Framework](#)". *Europa.eu*.
- 42 Hess, Mike; Ricart, Joan Enric (October 2002), "[Managing Customer Switching Costs: A Framework for Competing in the Networked Environment \(Working Paper\)](#)", IESE Working Paper.
- 43 "[Managing the Evolving Dynamics of Digital Platform Lock-In](#)". Boston Consulting Group. 2025.
- 44 Thiel, Peter (September 2014). "[Competition Is for Losers](#)". *The Wall Street Journal*. Retrieved January 21, 2026.
- 45 Rochet, Jean-Charles; Tirole, Jean (2004). "[Two-Sided Markets: An Overview](#)" (PDF). MIT.
- 46 Khan, L. M. (2017). "[Amazon's Antitrust Paradox](#)". *The Yale Law Journal*, 126(3), 710-805.
- 47 Doctorow, Cory (2025). *Enshittification: Why Everything Suddenly Got Worse and What To Do About It*. Verso Books.
- 48 Hill, Kashmir. "[Life Without the Tech Giants](#)". *Gizmodo*, January 22, 2019.
- 49 For example; PA Consulting (2023) "[PA Consulting expands Microsoft partnership to power AI transformation](#)".
- 50 Scott, T; Rung, A (2016) "[Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software](#)". Obama Whitehouse Archive.
- 51 Mazzucato, M, Collington, R (2023) *The Big Con: How the consulting industry weakens our Business, Infantilises our Governments and Warps our Economies*. Penguin. See chapter 7.
- 52 PwC. (January 2025). "[PwC and Microsoft announce strategic collaboration to transform industries with AI agents.](#)"
- 53 Microsoft. (July 2023). "[KPMG and Microsoft enter landmark agreement to put AI at the forefront of professional services.](#)"; Microsoft. (October 2025). "[KPMG International's strategic alliance with Microsoft is setting a new standard for auditing through digital transformation.](#)"
- 54 Deloitte. (n.d.). "[Microsoft Technology Services](#)". Deloitte. (May 2024). "[Deloitte named a global Leader in the IDC MarketScape for Microsoft Implementation Services.](#)"
- 55 Grant Thornton. (n.d.). "[Microsoft Alliance](#)"; Grant Thornton. (February 2024). "[Grant Thornton taps Microsoft technology to help clients manage compliance and risk using generative AI](#)"; Consulting.us. (2018, June 12). "[Grant Thornton partners with Microsoft to bring AI to federal agencies.](#)"
- 56 Parliamentary Joint Committee on Corporations and Financial Services. (2024). "[Ethics and Professional Accountability: Structural Challenges in the Audit, Assurance and Consultancy Industry](#)". Parliament of Australia.
- 57 Foley, S. (November 2025) "[SEC weighs looser independence rules for Big Four auditors](#)". *Financial Times*.
- 58 Opara-Martins, J., Sahandi, R., & Tian, F. (2016). "[Critical analysis of vendor lock-in and its impact on Cloud computing migration: a business perspective](#)". *Journal of Cloud Computing*, 5(1).
- 59 Statista. (February 2026) "[Worldwide market share of leading Cloud infrastructure service providers.](#)" Investopedia. (July 2025) "[The Cloud Computing Risk for the Economy That Many Don't See.](#)" Ternary. (January 2026) "[AWS vs. Azure vs. Google Cloud – Strengths, Differences, & More.](#)"

- 60 OECD. (June 2025) "[Competition in the Provision of Cloud Computing Services – Note by France](#)". DAF/COMP/WD(2025)21. Biglaiser, G., Crémer, J., de Cornière, A., & Mantovani, A. (January 2025). "[Should Egress Fees Be Eliminated? An Analysis of Cloud Services and Beyond](#)." CRESSE Conference 2025.
- 61 Jadotte, M., & Abeltino, G. (September 2025). "[The global harms of restrictive Cloud licensing, one year later](#)." Google Cloud Blog.
- 62 Competition and Markets Authority (July 2025) "[Final Decision Report](#)". Gov.uk.
- 63 Jenny, Pr. Frédéric (June 2023) "[Unfair Software Licensing Practices: A quantification of the cost for Cloud customers](#)" (PDF) CISPE.
- 64 Srnick, N (2025) *Silicon Empires*. Polity.Books, pp 22-31
- 65 For example, strageies are now being considered for processing on smaller devices on the edge of networks. See:Cai, G., Tian, R., Yang, L., Jia, Y., Li, L., & Wang, J. (2026). "[Efficient Inference for Edge Large Language Models: A Survey](#)." *Tsinghua Science and Technology*, 31(3), 1365-1380.
- 66 For example, Microsoft lobbied for 20 years to stop Linux and LibreOffice being used in Munich. They succeeded in 2023, although the policy was reversed back to gradual open source adoption a few years later. See Prakash, A (2023) "[Munich Is Ditching Linux For Purely Political Reasons](#)"; and Munich Open Source. "[Open Source in the Munich City Administration](#)"
- 67 Geoghegan, P, et al (September 2025) "[Blair and the Billionaire](#)". Lighthouse Reports.
- 68 Estgarth, P (2024) "[Personal announcement](#)". LinkedIn.
- 69 Colbert, M (July 2021) "[Revealed: The Involvement of Palantir and Faculty in the UK Public Sector](#)". *Byline Times*. Sinmaz, E (November 2020) "[Exposed: Dominic Cummings's links with two of the four companies detailed in damning PPE report](#)". *Daily Mail*. Mason, R., Dyer, H. (September 2025). "[Boris Johnson and Dominic Cummings had secret meeting with tech billionaire Peter Thiel](#)." *The Guardian*. Scott, Russell. (2025, October 31) [Dominic Cummings Lobbied Officials to Hand Test and Trace Contracts to Palantir After Secret Meeting with Peter Thiel](#). *Byline Times*. Fitzgerald, M., Crider, C. (December 2020). "[Controversial 'spy tech' firm Palantir lands £23m NHS data deal](#)". *OpenDemocracy*
- 70 Booth, R, Sabbagh, D. (February 2026) "[Mandelson's links with US tech firm Palantir must be fully exposed, campaigners warn](#)". *The Guardian*
- 71 "[Digital Markets, Competition and Consumers Act 2024](#)", legislation.gov.uk
- 72 Amin, L; Gheoghegan, P (June 2025) "[Revealed: "Shocking" scale of Big Tech's influence over Labour](#)". Democracy for Sale.
- 73 Shone, E. (October 2024). "[Revealed: No 10 adviser involved in AI policy has financial interests in AI](#)". OpenDemocracy.
- 74 Booth, R; Goodier, M (January 2026) "[Tech companies' access to UK ministers dwarfs that of child safety groups](#)". The Guardian.
- 75 Department of Business and Trade; Competition and Markets Authority (January 2025) "[Former Amazon boss named interim chair of CMA](#)". Gov.uk
- 76 Ring, S; Pickard, J (January 2025) "[Ousting of CMA chair prompts warnings of interference in UK regulation](#)". Financial Times.
- 77 Sandle, P; et al (January 2025) "[Britain appeals to Big Tech with change of regulatory guard](#)". Reuters.
- 78 Department for Business and Trade (May 2025) "[Strategic steer to the Competition and Markets Authority](#)". Gov.uk
- 79 Bordelon, B. (February 2024). "[AI doomsayers funded by billionaires ramp up lobbying](#)". *POLITICO*; Gebru, T., & Torres, É. P. (2024). "[The TESCREAL bundle: Eugenics and the promise of utopia through artificial general intelligence](#)." *First Monday*, 29(4).
- 80 Larrain, M. (2015). "[Trade Associations, Lobbying, and Endogenous Institutions](#)". *Journal of Law, Economics, and Organization*, 31(2), 467-504. Office of the United States Trade Representative. (2018). "[Industry Trade Advisory Committee on Services \(ITAC 10\) Report](#)".
- 81 UK Parliament, Public Administration and Constitutional Affairs Committee (2024) "[Parliamentary Scrutiny of International Agreements in the 21st century](#)". Second Report of Session 2023-24. London: House of Commons.
- 82 Fink, C., & Reichenmiller, P. (2006). "[Tightening TRIPS: Intellectual property provisions of US free trade agreements. In Trade, Doha, and Development: A Window into the Issues](#)" (pp. 291-308). World Bank.
- 83 Rosborough, A. (2025). "[Source code: A trade-related barrier to the right to repair](#)". Transatlantic Consumer Dialogue.
- 84 Larrain, M. (2015). "[Trade Associations, Lobbying, and Endogenous Institutions](#)". *Journal of Law, Economics, and Organization*, 31(2), 467-504. See "The rise of digital trade".
- 85 Milmo, D. (December 2025). "[Visa ban for European critics of online harm is first shot in US free speech war](#)". The Guardian.
- 86 See Greenleaf, Graham, (2018) "[Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108](#)" (November 30, 2018); Yakovleva, Svetlana and Irion, Kristina (2016) "[The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection](#)" (November 29, 2016); and Ruiz, Javier (2020) "[Briefing: how the UK-Japan trade deal severs post-Brexit data adequacy](#)". Open Rights Group.

- 87 Muro, M., & Methkuppally, S. (2025). ["Mapping the AI economy: Which regions are ready for the next technology leap"](#). Brookings Institution; Food & Water Watch. (2026). ["Artificial Jobs: The Illusion of Big Tech's Data Center Employment Claims"](#); show the concentration of high quality AI jobs in areas with software employment rather than datacentres.
- 88 Sutton, M. (May 2014). ["The Trans-Pacific Plague: How TPP Spreads the United States' Terrible DRM Policies"](#). Electronic Frontier Foundation; Transatlantic Consumer Dialogue. (December 2025). ["Taking Barriers to Access to Right to Repair Down: Transatlantic recommendations."](#)
- 89 Rosborough, A. D. (2020). ["Unscrewing the future: The right to repair and the circumvention of software TPMs in the EU"](#). Journal of Intellectual Property, Information Technology and E-Commerce Law, 11(1), 53-69.
- 90 Doctorow, C. (September 2020). ["Human Rights and TPMs: Lessons From 22 Years of the U.S. DMCA."](#) Electronic Frontier Foundation.
- 91 Rosborough, A. D. (2025) ["Source Code: A Trade-Related Barrier to the Right to Repair"](#). Washington DC: Transatlantic Consumer Dialogue.
- 92 Rangel, Daniel, and Lori Wallach. (February 2024) ["Trade Pacts Should Not Have Special Secrecy Guarantees for Source Code & Algorithms."](#) Tech Policy Press.
- 93 ["TSMC: lessons in strategy and operational excellence from the world's chipmaker"](#). IESE Insight. 1 (September 2025).
- 94 ["ASML Holding N.V.: The Indispensable Enabler of the AI Revolution"](#). PredictStreet. 30 September 2025.
- 95 Kerr, J., Garrett, M., & Bottomley, J. (October 2011). ["UEFI Secure Boot Impact on Linux, Red Hat and Canonical."](#)
- 96 Rutkowska, J. (October 2015). ["Intel x86 considered harmful"](#) (Version 1.0). Portnoy, E.; Eckersley, P (May 2017) ["Intel's Management Engine is a security hazard, and users need a way to disable it"](#). Electronic Frontier Foundation. Zammit, D. (June 2016) ["Recent Intel x86 processors implement a secret, powerful control system"](#). BoingBoing.
- 97 ["United States v. Microsoft Corp."](#)
- 98 ["Understanding the implications and risks of the US Cloud Act"](#). Claromentis. 2023-05-10.
- 99 Kunert, Paul (2025-07-25). ["Microsoft admits it 'cannot guarantee' data sovereignty"](#). The Register.
- 100 Boyle, Andrew (10 June 2021). ["Checking the President's Sanctions Powers"](#). Brennan Center for Justice.
- 101 Opere citato, p. 6.
- 102 Hsu, Spencer S. (24 June 2019). ["Chinese Bank Involved in Probe on North Korean Sanctions and Money Laundering Faces Financial 'Death Penalty'"](#). The Washington Post.
- 103 Boyle, opere citato, p.7. Vide etiam: US Department of the Treasury, Office of Foreign Assets Control. ["Basic Information on OFAC and Sanctions"](#).
- 104 Boyle, Adam; Lau, Tim (2021-07-20). ["The President's Extraordinary Sanctions Powers"](#). Brennan Center for Justice.
- 105 Boyle 2021, p. 9
- 106 Debusmann Jr, Bernd; Walker, Amy (6 February 2025). ["Dozens of countries back International Criminal Court after Trump sanctions"](#). BBC News.
- 107 ["International Criminal Court officials sanctioned by US"](#). BBC News. 2 September 2020.
- 108 Kania, Elsa B.; Laskai, Lorand (2021). ["Myths and Realities of China's Military-Civil Fusion Strategy"](#). Center for a New American Security.
- 109 Article 77, ["National Security Law of the People's Republic of China \(2015\)"](#). *China Law Translate*; Article 35 ["Data Security Law of the People's Republic of China \(2021\)"](#). *China Law Translate*. Retrieved 21 January 2026 and Article 7, 14 ["National Intelligence Law of the People's Republic of China \(2017, as amended 2018\)"](#). *China Law Translate*. Retrieved 21 January 2026.
- 110 Article 28, ["Cybersecurity Law of the People's Republic of China \(2016\)"](#). China Law Translate.
- 111 Opere citato, Article 37.
- 112 Article 18, ["Counter-Terrorism Law of the People's Republic of China \(2015, as amended 2018\)"](#). China Law Translate.
- 113 Kania & Laskai 2021, p. 13.
- 114 Kovacs, Eduard (26 June 2019). ["Many Potential Backdoors Found in Huawei Equipment: Study"](#). *SecurityWeek*.
- 115 ["Huawei Supply Chain Assessment"](#). Finite State. 26 June 2019.
- 116 Robertson, Jordan; Riley, Michael (12 February 2021). ["The Long Hack: How China Exploited a U.S. Tech Supplier"](#). *Bloomberg News*.
- 117 Auerbach, David (February 2015). ["You Had One Job, Lenovo"](#). *The Slate*.
- 118 Dos Santon, Nina; Greenwood, George (March 2024) ["Security fears over supercomputer deal with Chinese firm Lenovo"](#). *The Times*.
- 119 The company also claims high levels of security compliance, eg Lyons, Jessica (May 2024) ["68 tech names sign CISA's secure-by-design pledge"](#) *The Register*.
- 120 Clover, C (April 2025) ["UK bans EVs from some military bases over Chinese spy fears."](#) *Financial Times*.
- 121 Harrell, Peter (30 January 2025). ["Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology"](#). *Carnegie Endowment for International Peace*.
- 122 Hanton, A (2024) *Vassal State: How America Runs Britain*. Swift Press. See Chapters 4, 6 and 7 particularly.

- 123 Hüscher, P., & Williams-Dunning, S. (September 2025). "[A Big, Beautiful US Investment Boost for the UK Tech Sector?](#)" *Royal United Services Institute Commentary*.
- 124 ICON Corporate Finance (2025) "[UK M&A Review: AI – bubbling along nicely](#)".
- 125 Bradshaw, Tim (27 January 2014). "[Google buys UK artificial intelligence start-up](#)". *Financial Times*.
- 126 MacDonald, N, (26 July 2016) "[Arm's acquisition won't help our growth strategy](#)". *Financial Times*.
- 127 "[In the Matter of Nvidia/Arm: Case summary](#)". *Federal Trade Commission*. 14 February 2022.
- 128 See Appendix I for some of the most prominent examples
- 129 Ray, Bill (23 April 2008). "[Motorola unplugs Cambridge TTPCom unit](#)". *The Register*.
- 130 Puranam, P., & Srikanth, K. (2007). "[What they know vs. what they do: how acquirers leverage technology acquisitions](#)". *Strategic Management Journal*, 28(8), 805-825.
- 131 Shankland, S. (2013, September 3). "[Microsoft bolsters its patent access with Nokia deal](#)." *CNET*.; Mueller, F. (2013, September 3). "[1.65 billion euro patent licensing portion of Microsoft-Nokia deal validates Nokia's portfolio](#)." *FOSS Patents*.
- 132 Knowledge at Wharton. (2011, August 16). "[Google's Motorola Bid: Big Patent Portfolio – but Potentially Big Headaches, Too](#)."
- 133 Yang, J. (2014). "[The Use and Abuse of Patents in the Smartphone Wars: A Need for Change](#)." *Case Western Reserve Journal of Law, Technology & the Internet*, 5.
- 134 Statistics for the UK are difficult. For the EU, analysts conclude foreign direct investment to cause a reduced EU tax take. Gasparėnienė, L., Klietė, T., Šivickienė, R., Remeikienė, R., & Endrijaitis, M. (2022). "[Impact of Foreign Direct Investment on Tax Revenue: The Case of the European Union](#)." *Journal of Competitiveness*, 14(1).
- 135 Michel, B. (2024, November 6). "[Indicator deep dive: 'Royalties' and 'Services'](#)". Tax Justice Network.
- 136 Hanton, Angus (2024) "[Vassal State](#)". Swift Press, pp. 120-134.
- 137 European Investment Bank. (2026). "[Drivers of relocation by innovative EU startups and scaleups](#)."
- 138 House of Lords Communications and Digital Committee. (February 2025). "[UK risks becoming an 'incubator economy' if we don't take action to support our tech companies to scale up](#)." UK Parliament.
- 139 UK Government (2025) "[Cyber Security and Resilience \(Network and Information Systems\) Bill](#)" Parliament.uk
- 140 See Part 4 of the [Cybersecurity and Resilience Bill](#) for powers to compel access to source code.
- 141 Shipman, A (September 2017) "[The benefits of coding in the open](#)". GDS blog, Gov.uk
- 142 Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2008). "[An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure](#)". *Information Systems Research*.
- 143 Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). "[Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs](#)". *Journal of Cybersecurity*, 3(2), pp. 81-90.
- 144 Polo, N, Modhvardia, R (2025) [Great \(Public\) Expectations](#). Ada Lovelace. 89% of the public supported an independent regulator, 84% feared the government would prioritise relationships with AI companies over public concerns.
- 145 Charles III. (July 2024). [The King's Speech 2024](#). Gov.uk The Government would "seek to establish the appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models".
- 146 Clifford, M (January 2025). "[AI Opportunities Action Plan](#)." Gov.uk; and Department for Skills, Industry and Trade (January 2025) "AI Opportunities Action Plan: Government response". Gov.uk "Ensuring we have the right regulatory regime that addresses risks and actively supports innovation will drive trust and adoption across the economy. The government will set out its approach on regulation and will act to ensure that we have a competitive copyright regime that supports both our sector and the creative industries."
- 147 Science, Innovation and Technology Committee, House of Commons (December 2025) "[Oral evidence: Work of the Secretary of State for the Department for Science, Innovation and Technology, HC 1543](#)". *House of Commons*. See question 81: Liz Kendall: "It is not just an AI Bill; there are measures we will need to take to make sure we get the most on growth and deal with regulatory issues. If there are measures we need to do to protect kids online, we will take those. I am thinking about it more in terms of specific areas where we may need to act rather than a big all-encompassing Bill." Chair: "That sounds like a no."
- 148 Opere citato.
- 149 Kirkwood, M (July 2025) "[UK Deepens Dependence on US Tech with New OpenAI Partnership](#)" **Tech Policy Press**.
- 150 Kirkwood, M (October 2025) "[Despite Risks, the UK's Justice System Will Be Powered by ChatGPT](#)". Tech Policy Press.
- 151 For example, Online safety Coalition (2026) "[Strengthening the Online Safety Act: A 10 point Plan](#)" proposes means to strengthen the OSA, but does not set out measures that would change underlying market incentives; Molly Rose Foundation (2026) "[A Roadmap for a better online future](#)" proposes transparency measures and direction of funds from Big Tech to NGOs to research online harms, but does not contain market interventions that could change the underlying market dynamics. Similarly, the Center for Countering Online Hate propose a "STAR" framework, CCDH (2024) "[Building a Safe and Accountable Internet](#)" (Safety by Design, Transparency; Accountability and Responsibility). Accountability is framed as accountability to law and government, rather than to users; there are no measures proposed that would address market power or realign underlying business models with user needs or safety.

- 152 See discussion on CommuniTree for example. Seering, J. (2020). [“Reconsidering Self-Moderation: the Role of Research in Supporting Community-Based Models for Online Content Moderation”](#). Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), 1-28.
- 153 For example, through user switching and opening up content prioritisation engines. Kirkwood, Megan (2025) [“Making Platforms Accountable: Empowering users and creating safety”](#). Open Rights Group.
- 154 Loohuis, K (December 2025) [“Europe gets serious about cutting digital umbilical cord with Uncle Sam's big tech”](#). *The Register*.
- 155 <https://Cloud.google.com/sovereign-Cloud>
- 156 Grohmann, R., & Costa Barbosa, A. (2025). [“Sovereignty-as-a-service: How big tech companies co-opt and redefines digital sovereignty. Media, Culture & Society”](#).
- 157 Synopsys (2024) 2024 [Open Source Security and Risk Analysis Report](#). Synopsys, p. 4.
- 158 West, Joel (2003) [How open is open enough?: Melding proprietary and open source platform strategies](#). Research Policy, 32(7) 1259-1285, ISSN 0048-7333.
- 159 Parker, G., & Van Alstyne, M. (2018). [Innovation, Openness, and Platform Control](#). *Management Science*, 64(7), 3015–3032.
- 160 Greenway, A; Terrett, B.; Bracken, M; Loosemore, T (2021) [“Digital Transformation at Scale”](#). London Publishing Partnership. pp 15-16.
- 161 Carlberg, A. (January 2026) [“Open technologies, public procurement and economic impact: lessons from Denmark for Europe's next digital laws”](#). OpenForum Europe.
- 162 RedHat (ND) [“Our company”](#).
- 163 SUSE (ND) [“We are SUSE”](#)
- 164 Canonical (ND) [“Contact us”](#).
- 165 OpenEHR (ND) [“The future of digital health is open”](#)
- 166 X-Road (ND) [“The free and open-source data exchange solution”](#), managed by the Nordic Institute for Interoperability Solutions (NIIS), Estonia.
- 167 Matrix Foundation (ND) [“Members”](#). France's DINUM is a member alongside Open Source businesses and developers.
- 168 Cabinet Office (2025) [National Risk Register 2025](#)
- 169 Cabinet Office (2025) p. 19
- 170 See below, *Systems thinking and UK Digital Sovereignty*
- 171 Cabinet Office (2025) p. 18
- 172 Cabinet Office and Government Office for Science (2025) [“Chronic risk analysis”](#). Gov.uk
- 173 For example, Seifried, M., & Bertschek, I. (ZEW). (2021). *Schwerpunktstudie Digitale Souveränität* [Focus Study on Digital Sovereignty]. Federal Ministry for Economic Affairs and Energy (BMWi). Council for Technological Sovereignty / Federal Ministry of Education and Research (BMBF). (2025). *Impulse Paper: Strategically Securing Technological Sovereignty*, BMBF Ministry of Digital Affairs (Digitalisierungsministerium), Expert Group on Big Tech (Chaired by Prof. Mikkel Flyverbom). (2024). *The Role of Big Tech as Digital Infrastructure*. Digitalisierungsministerium;
- 174 <https://www.gov.uk/government/publications/industrial-strategy> p. 19
- 175 See for example the discussions at the German-French led Summit on European Digital Sovereignty <https://bmds.bund.de/aktuelles/eu-summit#c2021>, the 2025 summary at <https://www.elysee.fr/en/emmanuel-macron/2025/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe> and the industry-led initiative Eurostack <https://eurostack.eu/>
- 176 UK Government (2025). [“The UK's Modern Industrial Strategy.”](#) CP 1451. *Department for Business and Trade*. Presented to Parliament, November 2025. p. 8
- 177 Bailey, D., De Propriis, L., Dimos, C., Fai, F. M., Hardy, S., & Tomlinson, P. R. (2026). [“A critical review of the UK's Modern Industrial Strategy: lessons for 'place-based' policy.”](#) *Regional Studies*, 60(1).
- 178 Opere citato, p. 3
- 179 Opere citato, pp. 10-12
- 180 HM Government (June 2025) [“Digital and Technologies Sector Plan”](#) Gov.uk
- 181 HM Government. (January 2025). [“AI Opportunities Action Plan.”](#) GOV.UK.
- 182 HM Government. (September 2025). [“US-UK pact will boost advances in drug discovery, create tens of thousands of jobs and transform lives”](#). GOV.UK.
- 183 Department for Science, Innovation and Trade (July 2025) [“Memorandum of Understanding between UK and OpenAI on AI opportunities”](#). Gov.uk
- 184 HM Government (December 2025) [“Memorandum of Understanding between the UK and Google DeepMind on AI opportunities and security”](#). Gov.uk
- 185 HM Government (February 2025) [“Memorandum of Understanding between the UK and Anthropic on AI opportunities”](#) Gov.uk
- 186 Oracle. (September 2025). [“Oracle Continues to Deliver on \\$5B Investment Plans with New AI Capabilities for UK Government and Defence Organisations.”](#) Oracle United Kingdom.
- 187 HM Government (June 2025) [“Digital and Technologies Sector Plan”](#) Gov.uk
- 188 Financial Conduct Authority (2025). [“Open banking: a year of progress”](#). FCA.
- 189 CNBC. (22 January 2025). [“UK replaces CMA chair with ex-Amazon boss after anti-growth criticism”](#).
- 190 Booth, Robert; Milmo, Dan. (2025, January 22). [Competition watchdog role for ex-boss of Amazon UK 'a slap in face', say unions.](#) *The Guardian*.

- 191 Department for Business and Trade (May 2025) "[Strategic steer to the Competition and Markets Authority](#)". Gov.uk
- 192 Competition and Markets Authority. (10 October 2025). "[SMS investigation into Google's general search and search advertising services: Final decision report](#)". Gov.uk.
- 193 Competition and Markets Authority. (22 October 2025). "[CMA confirms Apple and Google have strategic market status in mobile platforms](#)". GOV.UK.
- 194 Competition and Markets Authority. (July 2025). "[Cloud services market investigation: final decision report](#)". Gov.uk, pp. 12, 15
- 195 Open Web Advocacy (March 2026) "[Our Submission to the CMA on Apple's iOS Interoperability Commitments](#)" OWA.
- 196 Collins, D (2026) "Foreword" in [Competitive Britain: the collective opt-out regime](#). Competitive Britain.
- 197 Department for Business and Trade (August 2025) "[Opt-out collective actions regime review: call for evidence](#)". Gov.uk
- 198 Speed, R. (December 2025) "[Here we go again: Microsoft in UK court over Cloud licensing](#)". The Register; Gerken, T. (December 2025) "[Microsoft faces £1bn class action case in UK over software prices](#)". BBC News. [Dr Maria Luisa Stasi v Microsoft Corporation, Microsoft Limited & Microsoft Ireland Operations Limited](#). 1696/7/7/24 Competition Tribunal.
- 199 Rahman-Jones, I (February 2024) "Facebook £3bn legal action given go-ahead in London". [Dr Liza Lovdahl Gormsen v Meta Platforms, Inc. and Others](#). 1433/7/7/22. Competition Tribunal.
- 200 Gerken, T. (June 2024) "[Court rules Google must face £13.6bn advertising lawsuit](#)". BBC News. [Ad Tech Collective Action LLP v Alphabet Inc. & Others](#). 1572/7/7/22; 1582/7/7/23 Competition Tribunal
- 201 See Hanton, A. (2024) *Vassal State*. Swift Press. Pp 31-38, for a general overview.
- 202 Cabinet Office (July 2025) "[Consultation on the NSI Act Notifiable Acquisition Regulations](#)". Gov.uk
- 203 Hogan Lovells. (2025). "[FDI Outlook 2025: Navigating National Security Reviews in a Transforming Global Landscape](#)". JD Supra.
- 204 Neuhaus, Kai (2026). "[CMS Expert Guide to Foreign Investment Screening Laws in Germany](#)". CMS
- 205 Ring, Suzi (January 2026) "[UK competition watchdog cleared every merger in 2025 after government pressure](#)", *Financial Times*.
- 206 Information Commissioners' Office (August 2025) "[ICO consultation on draft changes to how we handle data protection complaints](#)". [ico.org.uk](#)
- 207 Taylor, Diane, (November 2025) "[Civil liberties groups call for inquiry into UK data protection watchdog](#)". *The Guardian*. Open Rights Group (November 2025) "[70+ organisations and experts demand action over failing ICO](#)".
- 208 Delli Santi, M (2025) "[Analysis of the Draft UK Adequacy Decision](#)", Open Rights Group. See Chapter 5.
- 209 EU Commission (December 2025) "[C\(2025\) 8771 COMMISSION IMPLEMENTING DECISION amending Commission Implementing Decision \(EU\) 2021/1772 of 28 June 2021 pursuant to Regulation \(EU\) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom](#)" Europa.eu. See Chapter 6. Monitoring.
- 210 Thomas, D, Novik, M (January 2026) "[UK to outlaw non-consensual intimate images after Grok outcry](#)". *Financial Times*.
- 211 Kirkwood, Megan (2025) "[Making Platforms Accountable: Empowering users and creating safety](#)". *Open Rights Group*.
- 212 Wells, P. (2025) "[Consent Without Paying: Alternatives to Meta's Surveillance Advertising Models](#)". *Open Rights Group*; Dent, Anna (2025) "[Profiling by Proxy: How Meta's Data Driven Ads Fuel Discrimination](#)". *Open Rights Group*; Dr Riley, J. (2025) "[Bad Ads: Targeted Disinformation, Division and Fraud on Meta's Platforms](#)". *Open Rights Group*.
- 213 Information Commissioners Office (July 2025) "[ICO call for views on our approach to regulating online advertising](#)". [ico.org.uk](#); Delli Santi, M (September 2025) "[Notes from ORG Adtech Roundtable on the Future of Cookie Consent Requirements in the UK](#)". *Open Rights Group*
- 214 Delli Santi, M (January 2025) [ORG response to the ICO call for views on enforcement procedural guidance](#). Open Rights Group.
- 215 Cabinet Office, GDS (2025) "[State of digital government review](#)" Gov.uk
- 216 Department for Science, innovation and technology, Government Digital services (2025) [State of digital government review](#). Gov.uk
- 217 National Audit Office (2025) "[Government's approach to technology suppliers: addressing the challenges](#)" Gov.uk, p. 7
- 218 NAO 2024, p. 5
- 219 National Audit Office (2024) "[Government's approach to technology suppliers: addressing the challenges](#)" NAO, p. 6
- 220 See NAO re Cloud systems, p. 7
- 221 [Managing technical lock-in in the Cloud](#) (2025)[2019] gov.uk.
- 222 The UK has a process to manage open standards, through the [Open Standards Board](#) to ensure they are fully open, and not just 'developed in the open'. Some standards can exclude open source, by requiring limitations on the use of the code, adherence to patents, or other restrictions. See the UK's [Open Standards Principles](#).
- 223 [Open Source Software: Guidance on implementing UK Government Policy](#) (2002?) *Office of Government Commerce*.
- 224 Shipman, A. (2017) "[The benefits of coding in the open](#)". *Government Digital Services Blog*.
- 225 [Open Standards principles](#) (2019)[2012]

- 226 "Why you should use open standards", *ibid*.
- 227 "Open and interoperable data and software" in *The Digital, Data and Technology Playbook* (2023)
- 228 Sollof, Jordan (Dec 2025) "[NHS England quietly removes open source policy web pages](#)". Digital Health.
- 229 Ministry of Defence (ND) [Commercial X](#)
- 230 Pillai, Aingaran (Jan 2026) "[Fixing the foundation: Why investing in government commercial teams is the key to unlocking SME innovation](#)". TechUK.
- 231 European Commission, Directorate-General for Communications Networks, Content and Technology, (2021) "[The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy : final study report](#)." Publications Office. p.14
- 232 For the NHS, see for example Crider, Cory (2023) "Risk 5: monopoly lock-in", in *The NHS Federated Data Platform and Palantir: Seven Key Risks*. Foxglove and Doctors' Association UK.
- 233 Bambridge, J. (2025) "[Palantir lands biggest ever UK defense deal](#)". *Politico.eu*.
- 234 Various (2024) "[Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence](#)". Rand. p.68
- 235 Government Digital Service (June 2023). "[Government Cloud First policy](#)". *Gov.uk*,
- 236 "[Digital Marketplace](#)", *Gov.uk*.
- 237 Clark, L. (April 2024). "[UK gov office admits ability to negotiate billions in Cloud spending curbed by vendor lock-in](#)." *The Register*
- 238 GDS (2019) "[How the Home Office's Immigration Technology department reduced its Cloud costs by 40%](#)". *Gov.uk*.
- 239 Witzenberger, K., & Richardson, M. (2025, March 2). "[Microsoft cuts data centre plans and hikes prices in push to make users carry AI costs](#)". *The Conversation*.
- 240 Spataro, J (2021) "[New Pricing for Microsoft 365](#)". *Microsoft.com*
- 241 Clark, S (2021) "[Microsoft 365 price increase: How much will it affect you?](#)" *ThinkCloud.co.uk*
- 242 Treasure, L. (November 2021.). "[Microsoft 365 licensing and pricing changes coming](#)". *Chorus.co.uk*; Sereno Learning Hub. (2024). "[Microsoft global price increase 2023: What UK customers need to know](#)."
- 243 Shefford, T (ND) "[A Guide to the Microsoft Price Increase and License Renewals 2025](#)". *OpusTech.co.uk*
- 244 Gorton, J. (2025, December 8). "[Microsoft commercial price increases effective July 2026: UK-focused report](#)." *Bytes Technology Group*
- 245 Competition and Markets Authority. (2025, July 31). "[Cloud services market investigation: Summary of final decision](#)." GOV.UK.
- 246 Bang, B, Menon, H, Shepherd, J (July 2024) "[Clearing the air: Confronting the costs to Cloud adopters of restrictive software licensing practices](#)". Social Market Foundation.
- 247 Mansfield, A (January 2025) "[Microsoft and Google Are Forcing Customers to Adopt AI at a Premium Price: What Customers Need to Know](#)" *Upperedge.com*
- 248 Competition and Markets Authority (July 2025) "[Cloud services market investigation](#)". *Gov.uk*.
- 249 "whilst every organisation entering into contracts must be accountable for the agreements they purchase, Oracle places a disproportionate amount of risk and management overhead towards their customers". Thomson, M. (2014) "[Key Risks in Managing Oracle Licensing](#)" Campaign for Clear Licencing, p 16. Sjoerdsma, B. (2016). *Dealing with Vendor Lock-in*. University of Twente.
- 250 Clark, L. (July 2025). "[Capgemini wins £107M HMRC extension – no competition needed](#)". *The Register*. Butler, G. (June 2025). "[UK's HMRC signs £220m Fujitsu contract extension](#)". *Data Center Dynamics*. Clark, L. (2025, January 9). "[£3.8B later, old tech supplier flames still burning for HMRC](#)". *The Register*.
- 251 Horton, C. (December 2025,). "[A Decade After Breaking Up Big IT, UK Government Confronts New Digital Dependencies](#)". *THINK Digital Partners*.
- 252 Tussell (2025) "[Tussell Strategic Suppliers Report 2025](#)". Tussell. Figures derived from p. 17. Revenue is across all government spending tracked by Tussell.
- 253 A broad overview can be found in Rajala, T. & Aaltonen, H. (2021) "Reasons for the failure of information technology projects in the public sector" in *The Palgrave Handbook of the Public Servant*, Springer.
- 254 For the problems with non-competitive supplier markets, see Innes, A. (2025) *Late Soviet Britain: Why Materialist Utopias Fail*. Cambridge University Press. pp. 127-153 and Freedman, S. (2024) "Contract Killings" in *Failed State* Pan Macmillan. For t see also Mazzucato, M and Collington, R (2023) *The Big Con*. Penguin Books; especially chapter 4 on outsourcing and 10 Conclusion for the need for governments to reassert their own expertise.
- 255 Ross, M. (2018, July 9). "[The rise and fall of GDS: lessons for digital government](#)". Global Government Forum.
- 256 Foreshew-Cain, S. (2015). "[It's all about people: DVLA delivers real transformation](#)." Government Digital Service Blog.
- 257 Driver & Vehicle Licensing Agency (2016) "[Driver & Vehicle Licensing Agency Annual Report & Accounts: 2015–16](#)", GOV.UK, p. 8
- 258 Ross 2018
- 259 Nab L, Schaffer AL, Hulme W, et al. (2024) "[OpenSAFELY: A platform for analysing electronic health records designed for reproducible research](#)." *Pharmacoepidemiol Drug Safety*. 33(6):e5815.
- 260 Health Data Research UK (ND) "[Project: OpenSafely](#)"
- 261 OpenSafely (2025) "[About](#)".
- 262 Turnbull, G. (February 2025). "[How OpenSAFELY began](#)". *Bennett Institute for Applied Data Science*.

- 263 Black, C. (February 2021.). ["Revealed: Data giant given 'emergency' Covid contract had been wooing NHS for months."](#) The Bureau of Investigative Journalism.
- 264 Dunscombe, R (2024) ["Case Study: OpenEHR,"](#) OpenUK
- 265 Armstrong, S. (2023). ["Palantir gets £480m contract to run NHS data platform"](#). BMJ, 383, p2752.
- 266 Freedman, Sam (2024) ["Failed State"](#) PanMacmillan. p. 114-5
- 267 Freedman 2024 p. 114-5; Moore, A. (2024) ["Last Word: The UK's Destructive Love Affair with Outsourcing"](#) *Political Insight*, Vol. 15, Issue 1, pp. 40.
- 268 Ross 2018
- 269 Freedman 2024, pp. 54-7.
- 270 DSIT and GDS (January 2025) ["A blueprint for modern digital government"](#), Gov.uk
- 271 NAO 2025b, p. 11
- 272 Masley, N (ed) (2025) ["The 2025 AI Index Report"](#). Stanford University.
- 273 Robinson, S. (July 2025) ["Keeping the door open: A roadmap for integrating open-source AI in public services"](#). Social Market Foundation. p. 12.
- 274 The playbook advises that "When drafting requirements for AI, you should ... consider strategies to avoid vendor lock-in". Government Digital Services (2025) ["Artificial Intelligence Playbook for the UK Government"](#). Gov.uk
- 275 DSIT et alii (2020) ["Guidelines for AI procurement"](#). Gov.uk
- 276 ["Albert API: Fournir des services d'IA générative aux administrations"](#) beta.gouv.fr
- 277 ["Comparia: Interroger à l'aveugle deux modèles de langage conversationnels sur des tâches exprimées en français et comparer les résultats."](#) beta.gouv.fr
- 278 Chowdhury, Farzana (May 2025) ["Smarter Government, Powered by AI: What We Learned in France"](#). ai.gov.uk
- 279 Blackwell, J, Berman, J. (2025) ["The London Big Con"](#). Autonomy.work
- 280 Clark, Lindsay (September 2025) ["Europe's largest city council delays fix to disastrous Oracle system once more"](#). The Register.
- 281 Clark, Lindsay (February 2025) ["DXC paid 50% more than original contract value for disastrous public sector Oracle project"](#) The Register.
- 282 Clark, Lindsay (December 2025) ["Dorset Council ditching customized SAP for £14M Oracle overhaul"](#) The Register.
- 283 Local Government Society (2025) ["State of Digital Local Government"](#). See Market Concentration, and Note 5.
- 284 Hill, Nick (2026) ["Open Source Revenues & Benefits Solution"](#), Youtube. Quote from Steve Mawn at 44:47; councils cited at 52:40
- 285 <https://localgovims.digital/>
- 286 [Open Source Adult Social Care Video & Slidedeck](#), Public Sector Digital Transformation Forum.
- 287 Local Government Association (2025) ["State of Digital Local Government"](#).
- 288 Adams, L., & Blackwell, T. (November 2025). ["GDS Local goes live."](#) Government Digital Service.
- 289 Rumens, Phil (November 2025) ["Sourcing the stack for local government technology"](#) Gov.uk Technology blog.
- 290 Consul (ND) ["Scotland"](#).
- 291 Scottish Government. (2015). [Scotland's Digital Future: High Level Operating Framework Version 2.](#) PDF pp. 20-21, Ref OFP-CV4, OFP-CV5.
- 292 Davidson, A., & MacFarlane, T. (2015). [Scottish Sovereignty in the Age of Mass Surveillance: The Case for Open Source Procurement](#). Commonweal.
- 293 Scottish Government (2021) [Digital Scotland Service Standard](#); Hamilton, S (2021) ["Update to Digital First Service Standard"](#). Digital Blog, Gov.scot.
- 294 Scottish Government (2025) [Digital strategy for Scotland: vision statement](#).
- 295 Guthrie, Gordon (2024) [Foundations of the Digital State.](#); Fairless, B (2024) ["Foundations of the Digital State – Independent report published"](#). Digital Blog, Gov.scot.
- 296 Daley, T. (2026). [CDPS to join Welsh Government: time for a delivery-first evolution](#). Perago.
- 297 Kempster, A, Vaughan, D, Carter, J, Campbell, N (2025). [Transforming public services for a modern Wales](#). Transform Wales
- 298 OpenUK. (February 2024). [The Open Manifesto 2024](#). OpenUK.
- 299 OpenUK. (July 2023). [Open Source contributes £13.59 billion GVA to UK economy, finds OpenUK](#). Press Release. OpenUK.
- 300 Hoffmann, Mand Nagle, F and Zhou, Y, (2024) ["The Value of Open Source Software"](#) Harvard Business School Strategy Unit Working Paper No. 24-038.
- 301 Blind, K.; Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., Schubert, T. (2021). [The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy, Final Study Report](#). Brussels.
- 302 The Linux Foundation. (February 2026). [ROI for Open Source Software Contribution: Insight from the Open Source ROI Survey and Economic Model](#). The Linux Foundation.
- 303 Canonical (ND) ["Contact us"](#).
- 304 Collabora (ND) ["Contact Us"](#)
- 305 ["Raspberry Pi Ltd"](#). Companies House.
- 306 Element (ND) ["Company Information"](#).
- 307 HM Government (June 2025) ["Digital and Technologies Sector Plan"](#) Gov.uk

- 308 Cabinet Office (2025) [National Risk Register 2025](#) pp. 18-19. We have not analysed Future studies methodologies, but the same general points would likely apply.
- 309 Cabinet Office and Government Office for Science (2025) "[Chronic risk analysis](#)". Gov.uk
- 310 Ibidem, pp 33, 38.
- 311 Andreasiodmok (March 2020) "[Introducing a 'Government as a System' toolkit](#)".
- 312 Chapman, J (2004)[2002] [Systems failure: why governments must learn to think differently](#). Demos.
- 313 Jackson, MC (2024) [Critical Systems Thinking](#). Wiley. p. 40
- 314 Meadows, Donella H; Meadows, Dennis L; Randers, Jørgen; Behrens III, William W (1972). [The Limits to Growth: A Report for the Club of Rome's Project on the Predicament of Mankind](#). New York: Universe Books; pp 38-39
- 315 Andreasiodmok 2020
- 316 Government Office for Science (2023) [2020] [An introductory systems thinking toolkit for civil servants](#). Gov.uk
- 317 Ibidem.
- 318 Jackson 2024 p. 197.
- 319 Chapman 2004, p. 41, 74-77.
- 320 Jackson 2024 p.117, 134-141
- 321 Jackson, MC (2019) [Critical Systems thinking and the Management of Complexity](#). Wiley pp 435-441
- 322 Jackson 2024, p 99-100. Jackson 2019, pp. 490-502
- 323 Jackson 2024, p. 92-100.
- 324 Freedman, Sam (2024) "Enemies Within", *Failed State*. Pan Macmillan. pp 59-91.
- 325 Mazzacuto, M and Collington, R (2023) *The Big Con*. Penguin. See pp. 235-253.
- 326 Mazzacuto, M (2023) [2013] *The Entrepreneurial State*. Penguin. See Chapter 9 and 10 particularly.
- 327 Government Office for Science (2024) [2014] [Futures toolkit for policymakers and analysts](#). Gov.uk
- 328 See the [Open Source Observatory](#) for further examples.
- 329 The use of open source technologies for digital sovereignty is as of January 2026 the subject of a call for evidence at the EU <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom%3AAres%282026%2969111> and an EU consortium for joint open source infrastructure projects has also recently been formed <https://commons.ngi.eu/2025/10/30/dc-edic-the-eus-new-step-toward-a-sovereign-digital-infrastructure/>. See also Zenner, Kai et al, *The European Way. A Blueprint for Reclaiming Our Digital Future* (2025). <http://dx.doi.org/10.2139/ssrn.5251254>
- 330 Carlberg, A (2026) "[Open technologies, public procurement and economic impact: lessons from Denmark for Europe's next digital laws](#)." *Open Forum Europe*.
- 331 Blind, K., & Schubert, T. (2024). "[Estimating the GDP effect of Open Source Software and its complementarities with R&D and patents: evidence and policy implications](#)." *The Journal of Technology Transfer*, pp. 49, 466-491.
- 332 Synopsys Cybersecurity Research Center (CyRC). (2023). "[2023 Open Source Security and Risk Analysis Report](#)." *Synopsys, Inc.*
- 333 Ministry of the Interior and Kingdom Relations. (December 2025). [Vision on Digital Autonomy and Sovereignty of the Government](#). Rijksoverheid.
- 334 DINUM (2023) "[Le numérique au sein de l'État](#)". *Gouv.fr*
- 335 Federal Government of Germany (Scholz Government). (August 2022). "[Digital Strategy – Creating Digital Values Together](#)"; Presse- und Informationsamt der Bundesregierung. (November 2025). "[Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe](#)".
- 336 ZenDis (ND) "[Co-Coreating Digital Sovereignty](#)".
- 337 OpenDesk (ND) "[About](#)".
- 338 Examples include La Suite <https://lasuite.numerique.gouv.fr/en>
- 339 Nagle, Frank (2019) "[Government Technology Policy, Social Value, and National Competitiveness](#)". Harvard Business School Strategy Unit Working Paper No. 19-103,
- 340 "[Albert API: Fournir des services d'IA générative aux administrations](#)" beta.gouv.fr
- 341 [Welcome to EvalAP](#), gouv.fr
- 342 State Council of the People's Republic of China. (2017) "[New Generation Artificial Intelligence Development Plan](#)." Translated by Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo. Stanford DigiChina, August 1, 2017.
- 343 Meinhardt, Caroline, Sabina Nong, Graham Webster, Tatsunori Hashimoto, and Christopher Manning. "[Beyond DeepSeek: China's Diverse Open-Weight AI Ecosystem and Its Policy Implications](#)." Stanford HAI Policy Issue Brief, December 16, 2025.
- 344 Chan, Kyle, Gregory Smith, Jimmy Goodrich, Gerard DiPippo, and Konstantin F. Pilz. (June 2025) "[Full Stack: China's Evolving Industrial Policy for AI](#)." RAND Corporation Expert Insights.
- 345 O'Brien, C. (January 2026,). "[French Tech Startup Funding 2025: €8.2B Raised As AI Took 62%](#)". The French Tech Journal; Leprince-Ringuet, D. (November 2024, November). "[The origins of the French tech boom – and what's still to come](#)." Sifted.
- 346 Bradshaw, T. (February 2026) "[Mistral's revenues soar over \\$400mn as Europe seeks AI independence](#)". *Financial Times*.
- 347 <https://eurollm.io/>
- 348 OpenEuroLLM (2025) "[Open LLMs for Transparent AI in Europe](#)".
- 349 ETH Zurich (September 2025) "[Apertus: a fully open, transparent, multilingual language model](#)"

- 350 Jenny, Pr. Frédéric (June 2023) "[Unfair Software Licensing Practices: A quantification of the cost for Cloud customers](#)" (PDF) CISPE.
- 351 EUCOM (2025) "[Digital Package](#)".
- 352 European Digital Rights (November 2025) "[Forthcoming Digital Omnibus would mark point of no return](#)".
- 353 Eclipse Foundation & DECISION. (2023). "[Unlock the Cloud Interoperability to Foster the EU Digital Market](#)."
- 354 CISPE. (2025). "[CISPE Sovereign Cloud Manifesto](#)."
- 355 Bauer, M., & Pandya, D. (December 2025). "[Europe's Cloud Debate Is Looking the Wrong Way: It's Not Concentration – It's Lock-In](#)." ECIPE.
- 356 European DIGITAL SME Alliance. (September 2025). "[Strategic buying for Europe: A mission-oriented vision on public procurement](#)."
- 357 CISPE. 2025, p. 4
- 358 European Commission Digital Directorate (October 2025) "[Cloud Sovereignty Framework](#)". Europa.eu
- 359 Hubert, B (May 2025) "[A coherent European/non-US Cloud strategy: building railroads for the Cloud economy](#)". Bert Hubert's writings.
- 360 CISPE 2025, p. 8
- 361 CISPE 2025, p. 7
- 362 France 2030 (February 2025) "[IA : une nouvelle impulsion pour la stratégie nationale](#)". Gouv.fr
- 363 Fermigier, S. (February 2026) "[Gaia-X – Chronicle of a Failure Foretold](#)". Eurostack.
- 364 Hofer, P., & Herzwurm, G. (2024). "[From Compliance Risk to Business Model – Cloud Sovereignty as a Door Opener for the EU Market](#)." In *International Conference on Digital Product Management*. Springer
- 365 Burwell, F, Propp, K. (January 2026). "[Digital sovereignty: Europe's declaration of independence?](#)" Atlantic Council.
- 366 Évroux, C, Hallak, I (December 2025) "[Briefing: The 28th regime](#)". European Parliament
- 367 Rankin, J (February 2026) "[EU leaders agree to move ahead with 'Buy European' policy](#)". The Guardian.
- 368 "[L'espace de travail ouvert et souverain des agents de l'État](#)". Gouv.fr
- 369 Vaughan-Williams, S. (January 2026) "[Why France just dumped Microsoft Teams and Zoom – and what's replacing them](#)" ZDNet.
- 370 Element (ND) "[France embraces Matrix to build Tchapp](#)". Element.io; Matrix Foundation (ND) "[Members](#)". Matrix.org
- 371 "[NATO NI2CE Messenger builds on Matrix](#)" Element.io
- 372 "[TI-Messenger – Interoperables Instant Messaging im Gesundheitswesen](#)" gematic Fachportal
- 373 <https://www.zendis.de/en>
- 374 <https://www.opendesk.eu/en/>
- 375 <https://www.zendis.de/en/what-we-offer#consulting>
- 376 Pätsch, S. (April 2025) "[BWI/Bundeswehr Chooses Open Source by Adopting openDesk](#)" InteroperableEurope.
- 377 Daxhelet, E. (August 2025) "[German Public Health Service Migrates to Open Source with openDesk](#)". InteroperableEurope.
- 378 Krempf, S (January 2026) "[Microsoft alternative: Social insurers trial OpenDesk for emergencies](#)". Heise.de
- 379 Günther, C. (November 2025) "[OpenProject at the Berlin Summit on European Digital Sovereignty](#)". OpenProject blog.
- 380 Voss, L (November 2025) "[International Criminal Court switches to open source with openDesk](#)" Open Source Observatory.
- 381 Ville de Lyon (June 2025) "[La Ville de Lyon renforce sa souveraineté numérique](#)".
- 382 Fermigier, Stefane (March 2025) "[Schleswig-Holstein's Bold Open Source Leap: A Model for Digital Sovereignty?](#)" EuroStack. Tonekaboni, K, Wölbart, C (February 2025) "[Von Microsoft zu Open Source: Wie Schleswig-Holstein den Wechsel schaffen will](#)" Heise.de
- 383 Bierhals, G (ND) "[Towards the freedom of the operating system: The French Gendarmerie goes for Ubuntu](#)". Interoperable Europe; Vaughan-Williams, S. (June 2025) "[Yet another European government is ditching Microsoft for Linux – here's why](#)" ZDNet.
- 384 Vignoli, I (March 2025) "[BIG NEWS: Germany has just made the standard Open Document Format \(ODF\) mandatory](#)" Open Document Foundation Blog
- 385 Digwatch (June 2025) "[Denmark moves to replace Microsoft software as part of digital sovereignty strategy](#)"; Jones, S (June 2025) "[Denmark Steps Up Push for Digital Sovereignty](#)". TechStory. Carlberg, A. (January 2026) "[Open technologies, public procurement and economic impact: lessons from Denmark for Europe's next digital laws](#)". OpenForum Europe.
- 386 Open Government. (March 2025). "[Building the Workplace of the Future with Open Source](#)".
- 387 Plantera, F. (2019, March 20). "[The business registers of Estonia and Finland start cross-border interoperability](#)". X-Road Blog. Nordic Institute for Interoperability Solutions. (2026). [X-Road Source Code Repository](#). GitHub. X-Road (ND). [X-Road Technology Overview](#).
- 388 [X-Road Factsheet](#), (PDF) e-estonia.com
- 389 "[X-Road World Map](#)"
- 390 [Nordic Institute for Interoperability Solutions](#)
- 391 [European Digital Identity Project](#), Github. EU Commission (ND) "[A digital ID and personal digital wallet for EU citizens, residents and business](#)". Europa.eu
- 392 Nordic Institute for Interoperability Solutions (December 2024) "[Making of X-Road 8 – December 2024 Status Update](#)", Niis.org
- 393 "[The MOSIP Project](#)", mosip.io

- 394 Martin, A. (2021). "[Aadhaar in a box? Legitimizing digital identity in times of crisis.](#)" *Surveillance & Society*, 19(1), 104-122.
- 395 For example, see this discussion on anonymisation and the potential for producing Open Data: Kak, A., Parsheera, S., & Kotwal, V. (2017). "[Open data and digital identity: Lessons for Aadhaar.](#)" *National Institute of Public Finance and Policy*.
- 396 As well as official audits, there is independent analysis, for example, Bakhtina, M., Leung, K. L., Matulevičius, R., & Awad, A. (2023). "[A Decentralised Public Key Infrastructure for X-Road.](#)" In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-11). ACM; or Priisalu, J and Ottis, R. (2017). "[Personal control of privacy and data: Estonian experience.](#)" *Health Technology*, 7(4), 441-451.
- 397 European Central Bank (November 2025) "[The digital euro: key aspects at a glance](#)" (PDF) payments should be "at full face value: any reductions from full face value need to be limited and justified; PSPs [payment services providers] should be adequately compensated for related costs"; Bank of England (ND) "[The Digital Pound](#)". "What could I use my digital pounds for? ... These innovations could change the way people pay, making it faster and less expensive."
- 398 Belli, L. (2024). "[Building Good Digital Sovereignty Through Digital Public Infrastructures And Digital Commons In India And Brazil.](#)" FGV Law School Rio de Janeiro, CyberBRICS Project.
- 399 Modern Diplomacy. (September 2025). "[Brazil's Pix and the Geopolitics of Digital Payments.](#)"
- 400 Wero (ND) [Shop online with Wero](#). Wero Wallet.eu
- 401 Tamma, P (February 2026) "[Mastercard 'urgently' needed, says banking chief](#)". *Financial Times*. See also [EPI website](#).
- 402 Makortoff, K (February 2026) "[UK bank bosses plan to set up Visa and Mastercard alternative amid Trump fears](#)". *The Guardian*.
- 403 Paton, C., Braa, J., Muhire, A., Marco-Ruiz, L., Kobayashi, S., Fraser, H., Marcelo A. & Falcón, L. (2022). [Open Source Digital Health Software for Resilient, Accessible and Equitable Healthcare Systems: Contribution from the IMIA Open Source Working Group](#). *Yearbook of Medical Informatics*, 31(1), pp. 67–73. p. 69
- 404 Mohammed-Rajput, N. A., Smith, D. C., Mamlin, B., Biondich, P., & Doebbeling, B. N. (2011). OpenMRS, A Global Medical Records System Collaborative: Factors Influencing Successful Implementation. *AMIA Annual Symposium Proceedings, 2011*, 960–968. PMID: PMC3243141; Syzdykova, A., Malta, A., Zolfo, M., Diro, E., & Oliveira, J. L. (2017). [Open-Source Electronic Health Record Systems for Low-Resource Settings: Systematic Review](#). *JMIR Medical Informatics*, 5(4), e44.
- 405 GNU Solidario, "[About us](#)".
- 406 <https://openimis.org/impact>
- 407 Ministère de l'Éducation nationale et de la Jeunesse. (2023). [Stratégie du numérique pour l'éducation 2023-2027](#). p.33 Machine translation.
- 408 Eurydice (June 2025) [France: New tools for teaching thanks to artificial intelligence](#).
- 409 DataEthics.eu. (2024, June 18). [How France Adopts An Open Source-Based Education Strategy - Free of Big Tech](#).
- 410 Rédaction, « [Souveraineté : la France championne du monde Nextcloud avec 1.2 million d'utilisateurs \[archive\]](#) », sur Goodtech, via [French Wikipedia](#).
- 411 Interoperable Europe Portal. (2021). [The use of open source cloud in education: Cases of HPI Schul-Cloud and Sciebo in Germany](#).
- 412 DPA (2021) [Schul-Cloud des HPI mit über einer Million Nutzern](#). *Süddeutsche Zeitung*
- 413 See <https://blog.e-learning.tu-darmstadt.de/2010/04/09/moodle-instancen-an-deutschsprachigen-hochschulen/#comment-1904>
- 414 <https://moodle.org/>
- 415 Nextcloud. (2022). [Data protection: Microsoft 365 banned in Baden-Württemberg's schools – suitable alternatives exist](#).
- 416 SURF.nl. (2025). [Onderwijs en onderzoek gaan verder met Nextcloud](#).
- 417 Kennisnet. (n.d.). [Wikiwijs: Zoek open lesmateriaal](#).
- 418 European Data Protection Board. (2022). [The Danish DPA imposes a ban on the use of Google Workspace in Elsinore Municipality](#). OS2skole. (n.d.). [OS2skole](#).
- 419 Tranberg, P (2025) [New Open Source-Based Platform Can Disrupt Big Tech's Grip on Danish Schools](#). Dataethics.eu.
- 420 Open Contracting Partnership (ND) "[The Open Contracting Data Standard](#)". *Open Contracting*.
- 421 Tarnay, V, Dmytryshyn, Y (December 2024) "[How to make better public procurement decisions with business intelligence: Insights from Ukraine](#)". *Open Contracting*.
- 422 UN (2018) "[Initiative: Citizen Participation Project](#)"
- 423 Consul Democracy, [Decide Madrid \(case study\)](#).
- 424 See [map](#).
- 425 <https://decidim.org/>
- 426 Miller, Carl. "[How Taiwan's 'civic hackers' helped find a new way to run the country](#)". *The Guardian*.
- 427 <https://www.digitalpublicgoods.net/roadmap>
- 428 Digital Public Goods Alliance. (2021). "[2021 DPGA Annual Report](#)".
- 429 Ministry of Foreign Affairs (September 2025) "[France joins the Digital Public Goods Alliance to promote an inclusive and equitable digital future](#)", [diplomatie.gouv.fr](#)
- 430 Gates, Nicholas (May 2025) "[Europe's Digital Public Goods Moment: New Use Cases for Public Sector Adoption of DPGs in Europe](#)". EU Open Source Observatory.

- 431 Open Government Partnership. "[About Open Government Partnership](#)" OGP; US Department of State (2011) "[The Open Government Partnership](#)", US archive.
- 432 United Nations (May 2025) "[France Becomes First Government To Endorse UN Open Source Principles](#)", UN.
- 433 <https://interoperable-europe.ec.europa.eu/>
- 434 <https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor>
- 435 Sharma, Shreyas (February 2025) "[RISC-V vs ARM: A Comprehensive Comparison of Processor Architectures](#)" *Wevolver*.
- 436 Shivakumar, Sujai and Heng, Julie (April 2025) "[Sustaining Standards Leadership: The United States Cannot Disengage from RISC-V](#)". Centre for Strategic and International Studies.
- 437 SiFive (2021) "[SiFive and DARPA collaborate to bring the power of RISC-V to Technology Innovation](#)"
- 438 Frazzoli, Roberto (2025) "[A Brief Overview of the EU Chips Act](#)", *Embedded*.
- 439 Mordor Intelligence [RISC-V Tech Market Share, Size & Growth Outlook to 2031](#)
- 440 EU Commission (January 2025) "[European Open Digital Ecosystems: About this initiative](#)". *Europa.eu*
- 441 Singh, A, Tarkowski, A (February 2026) "[European Digital Ecosystems and Digital Commons](#)". *OpenFuture blog*.
- 442 Maris, J (March 2025) "[Feedback from Open Source Initiative](#)". *Europa.eu*
- 443 Sovereign Tech Agency (ND) "[Sovereign Tech Fund](#)", "[Sovereign Tech Resilience](#)"
- 444 Gates, N et alii (2025) "[Funding Europe's Open Digital Infrastructure](#)". OpenForum Europe.
- 445 Chee, FY (March 2025) "[Airbus leads call for Europe to create sovereign infrastructure fund, buy European](#)". *Reuters*.
- 446 Open Source Initiative (2024)[2006] [Open Source Definition](#).
- 447 Smith, McCoy (December 2025) "[Patents and Open Source: Understanding the Risks and Available Solutions](#)". Open Source Initiative.
- 448 Carugati, C (2024-) "[European Digital Competition Regime tracker](#)." *Digital Competition by Dr C Carugati*.
- 449 BEUC (November 2025) "[First bloom: consumer choice after eighteen months of the Digital Markets Act](#)". (PDF) *BEUC.EU*. EU Commission (January 2026) "[Commission opens proceedings to assist Google in complying with interoperability and online search data sharing obligations under the Digital Markets Act](#)". *Europa.eu*
- 450 Meta. (November 2025). [Messaging Interoperability: WhatsApp enables third-party chats for users in Europe](#). Meta Newsroom. Meta for Developers. (ND). [Messaging Interoperability](#). BEREC. (March 2025). [BEREC pinion on Meta's reference offers to facilitate Messenger and WhatsApp interoperability under Article 7 of the Digital Markets Act](#).
- 451 European Data Protection Supervisor. (April 2022). [EDPS launches pilot phase of two social media platforms](#). European Commission. (n.d.). [European Commission on Mastodon](#).
- 452 social.bund.de. (n.d.). [social.bund.de](#).
- 453 Sovereign Tech Agency. (n.d.). [ActivityPub Test Suite](#). Sovereign Tech Agency. (n.d.). [Fedify](#).
- 454 Hate Aid (2025) "[Safety by Design](#)"
- 455 Panopytkon (February 2026) "[DSA vs. Reality: Are children safer online?](#)"
- 456 Article 19 (June 2021) "[Digital Markets Act: Civil Society addresses the European Parliament \(IMCO\)](#)"
- 457 Bundeskartellamt. (2024). [Facebook proceeding concluded](#). Court of Justice of the European Union. (2023). [PRESS RELEASE No 113/23](#).
- 458 Bundeskartellamt (ND) [Rules for the digital economy](#)
- 459 For example, see Wörsdörfer, M. (2023). "[The Digital Markets Act and EU competition policy: A critical ordoliberal evaluation](#)". *Philosophy of Management*, Springer.
- 460 Claassen, R. & Gerbrandy, A. (2016). "[Rethinking European Competition Law: From a Consumer Welfare to a Capability Approach](#)". *Utrecht Law Review*, 12(1), 1-15. Gerbrandy, A., Morozovaitė, V. & Phoa, P. (2025). "[Power in a Digitalised World: Evolving Perspectives on Competition Law, Regulation and Beyond](#)". *Utrecht Law Review*, 21(2), 1-4.
- 461 On the need for institutions, see Pope, Richard (2024) [Platformland: An anatomy of next-generation public services](#). pp. 213-236
- 462 Gates, N (OFE), Yannis Chourmouziadis, Y & Johan Linåker, J (2025) "[Open Source Software Adoption and Reuse in European Local Governments: A Multiple-Case Study](#)". *Open Forum Europe*.
- 463 Canonical (ND) "[Contact us](#)".
- 464 Collabora (ND) "[Contact Us](#)"
- 465 "[Raspberry Pi Ltd](#)". *Companies House*.
- 466 Element (ND) "[Company Information](#)".
- 467 European Commission Digital Directorate (October 2025) "[Cloud Sovereignty Framework](#)". *Europa.eu*
- 468 Pope 2024, pp. 213-236
- 469 Massoudi, A (18 July 2016) "[SoftBank to acquire UK's Arm Holdings for £24.3bn](#)". *Financial Times*.
- 470 MacDonald, N, (26 July 2016) "[Arm's acquisition won't help our growth strategy](#)". *Financial Times*.
- 471 "[In the Matter of Nvidia/Arm: Case summary](#)". *Federal Trade Commission*. 14 February 2022.
- 472 Sweney, Mark; Agency Staff (8 February 2022). "[Nvidia's \\$40bn takeover of UK chip designer Arm collapses](#)". *The Guardian* and Sweney, Mark (3 March 2023). "[UK chip designer Arm chooses US-only listing in blow to Rishi Sunak](#)". *The Guardian*.
- 473 Sayer, Peter (22 July 2025). "[The HP-Autonomy lawsuit: Timeline of an M&A disaster](#)". *CIO*.
- 474 Sword, Alexander (18 July 2016). "[6 of the biggest UK tech acquisitions by overseas giants](#)". *TechMonitor*.
- 475 Cellan-Jones, Rory (2 January 2020). "[Imagination announces new Apple licence deal](#)". *BBC News*.
- 476 Bradshaw, Tim (27 January 2014). "[Google buys UK artificial intelligence start-up](#)". *Financial Times*.
- 477 Sword 2016

478 Ray, Bill (23 April 2008). ["Motorola unplugs Cambridge TTPCom unit"](#). *The Register*.

479 Sword 2016

480 Tussell 2025

481 Tussell 2025

482 Clark, L. (2025, January 9). ["£3.8B later, old tech supplier flames still burning for HMRC"](#). *The Register*.

483 Clark, L. (November 2023). ["Brit pensions scheme flushed £74M when it walked from Atos deal"](#). *The Register*.

484 Atos. (December 2021). ["Atos selected as HMRC agile transformation delivery partner"](#) Atos. (March 2022). ["Atos wins contract with HMRC to enhance its capabilities with critical testing services."](#)

485 Clark, L. (March 2025) ["Troubled French outsourcer Atos finds pot of gold at the end of UK state bank Rainbow"](#). *The Register*.

486 Competition and Markets Authority (July 2025) ["Cloud services market investigation"](#). *Gov.uk*

487 Clark, L. (December 2025) ["UK govt office admits ability to negotiate billions in Cloud spending curbed by vendor lock-in"](#). *The Register*.

488 Greasley, S. (2019). ["Mutual dependence or state dominance? Large private suppliers and the British state 2010–15"](#). *Public Administration*, 97(2), 433-448.

489 National Audit Office. (2025). ["Investigation into the administration of the Civil Service Pension Scheme"](#) (HC 951, Session 2024-25). London: National Audit Office.

490 Peachey, Kevin. (February 2026) ["Civil service pension backlog 'overwhelmed' Capita, boss says"](#). BBC News.

491 Clark, L. (July 2025). ["Capgemini wins £107M HMRC extension – no competition needed"](#). *The Register*.

492 Weale, S, Adams, R (January 2021) ["Malware reportedly found on laptops given to children in England"](#). *The Guardian*.

493 Williamson, B., Hogan, A., & Eynon, R. (2021). ["Covid-19 controversies and critical research in digital education"](#). *Learning, Media and Technology*, 46(2), 117-127.

494 CGI. (November 2025). ["CGI awarded £250 million Enterprise Integration Services contract with His Majesty's Revenue & Customs UK."](#)

495 Technology Reseller. (2022, October 11). ["Home Office contract win for CGI."](#)

496 Haynes, D. (October 2017). ["Computer upgrade for MoD is £900m fiasco"](#). *The Times*.

497 Kunert, P. (November 2017). ["Oh dear, DXC: Outsourcer loses two UK.gov contracts"](#). *The Register*.

498 Clark, L. (February 2025). ["DXC paid 50% more than original contract for Oracle project."](#) *The Register*.

499 Butler, G. (June 2025). ["UK's HMRC signs £220m Fujitsu contract extension"](#). *Data Center Dynamics*.

500 Trendall, S. (June 2025) ["Government stresses 'limited time and strict terms' as HMRC signs £220m Fujitsu contingency extension"](#). *Public Technology*.

501 Clark, L. (July 2025) ["Fujitsu sorry for Post Office horror – but still cashing big UK govt checks"](#). *The Register*.

502 Flinders, K (April 2023). ["Post Office paid IBM millions when it ended proposed contract to replace Horizon."](#) *Computer Weekly*.

503 Public Accounts Committee. (July 2023). ["Significant costs to emergency services caused by Home Office failures on communications network."](#) *UK Parliament*.

504 National Audit Office. (November 2025). ["National Savings & Investments' Business Transformation Programme"](#) *HC 1379, Session 2024-2026*.

505 Rose, A.(November 2025). ["MPs slam £700 million NHS deal, accuse Microsoft of overcharging"](#). *EasternEye*.

506 Clark, Lindsay (December 2025) ["UK eyes more tech megadeals after Microsoft pact"](#). *The Register*.

507 Nagle, Z., & White, S. (December 2025). ["Microsoft 365 2026 Price Increase: How to Defend Your Budget."](#) Gartner; Bytes. (December 2025). ["Microsoft Commercial Price Increases Effective July 2026 \(UK-Focused Report\)"](#).

508 Witzemberger, K., & Richardson, M. (2025, March 2). ["Microsoft cuts data centre plans and hikes prices in push to make users carry AI costs"](#). *The Conversation*.

509 Clark, Lindsay (September 2025) ["Europe's largest city council delays fix to disastrous Oracle system once more"](#). *The Register*.

510 Haynes, J (February 2025) ["Red flags ignored as Birmingham City Council IT fiasco failure exposed in damning report"](#). *Birmingham Mail*.

511 Clark, Lindsay (February 2025) ["DXC paid 50% more than original contract value for disastrous public sector Oracle project"](#) *The Register*.

512 Donnelly, C. (October 2024) ["Oracle and IBM clinch 10-year cross-departmental Cloud deal with UK government"](#). *Computer Weekly*

513 DuPreez, D. (August 2019, A). ["Sopra Steria promised a 'streamlined' digital visa service for students – what they got is 'woefully inadequate'."](#) *Diginomica*. Bulman, M. (June 2019). ["MPs call for investigation into privatised visa system after applicants charged 'disgraceful' fees."](#) *The Independent*

514 House of Commons Committee of Public Accounts (2023) ["Investigation into the UK Passport Office"](#) Forty-Seventh Report of Session 2022–23, HC 738.

515 Weston, S. (November 2020) ["Sopra Steria cyber attack costs to hit €50 million"](#) *ITPro*.

516 Corfield, G. (October 2020) ["We couldn't deliver prisoner rehab plans because Sopra Steria ballsed up our IT, Interserve tells High Court"](#) *The Register*.