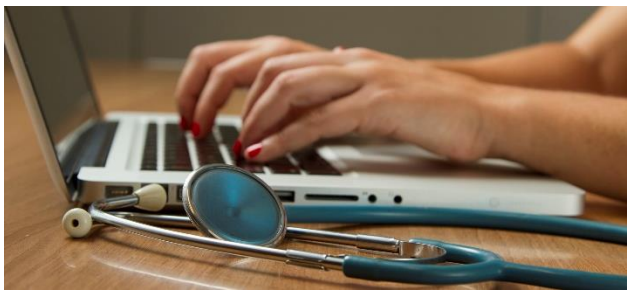
UK Parliament POST

POSTNOTE

Number 664

Sharing Public Sector Data



Public sector data can be used to improve services, facilitate research and innovation, and inform policymaking. This POSTnote looks at how public sector data is shared between public sector bodies and with researchers and private organisations in the UK. It looks at requirements for effective data sharing and discusses the associated risks and barriers.

Overview

- In its 2020 National Data Strategy, the Government outlined plans to increase the societal and economic benefits of data, including through improved data sharing.
- In September 2021 it proposed changes to the UK's data protection regime, which would affect public sector data sharing.
- Challenges to public sector data sharing include: cultural and skills barriers; poor data quality; a lack of public trust; and security and privacy concerns.
- Many experts say better guidance, more transparency and use of data intermediaries may address the challenges.

Background

Public sector data refers to information generated and collected by public sector bodies, such as government departments, local authorities, police forces, the NHS, and schools.[1,2] Data are used to run public services, monitor trends, and understand the population's needs. Examples of public sector data include:[1]

- personal data or records about people generated through interaction with public services, such as individuals' names or the outcomes of hospital appointments
- population level data and statistics, such as that collected through birth and death registrations[3]
- administrative, operational, and transactional data, such as tax records or procurement expenditure[4]
- infrastructure, geospatial and environmental data.[5–7]

It is widely agreed that sharing good quality public sector data, both within the public sector and externally, can improve public sector services and benefit the economy and society.[8–12] However, risks and barriers associated with sharing public sector data persist.[13–17]

The key pieces of UK legislation that apply to the sharing of public sector data are the Data Protection Act 2018, UK GDPR, and the Digital Economy Act 2017 (Box 1). Once a legal basis for sharing data has been established data can be shared by:

- direct data transfer between organisations, often through dedicated data sharing platforms[18]
- providing secure points where data can be accessed for analysis, without sharing a copy of the data[19,20]
- publishing data so they are publicly available.[8]

Many stakeholders, including the Government, have highlighted that public sector data are not shared effectively and that their value is currently underexploited.[8–12] In September 2020, the Government published its National Data Strategy (NDS, Box 1 2) setting out plans to "unlock the power of data" in the UK, including the role and opportunities for public sector data.[1] In September 2021, the Government opened a consultation on its proposals to reform the UK's data protection regime, which would affect sharing of public sector data (Box 3).[21–23]

Public sector data sharing in practice

Public sector bodies share data with each other or with external organisations for a variety of purposes, such as to detect fraud, identify vulnerable people, or build infrastructure.[24,25] Public bodies may share data with contractors (e.g. to deliver IT services),[26] or with researchers.[27] Some public bodies make data freely available for anyone to access. Transport for London makes data on transport use publicly available, which Deloitte estimated adds up to £130m per year to London's economy, mostly via privately developed journey-planner apps.[28]

Benefits

The wider economic value of public sector data is challenging to measure.[8,29] However, a 2013 Government-commissioned assessment of public sector data estimated its value to the UK economy at £1.8 billion.[30] Sharing data between public sector bodies also has societal benefits, such as the ability to identify vulnerable individuals and families. For example, the 'child protection information sharing project' facilitates data sharing between social services and parts of the NHS to assess a child's

The Parliamentary Office of Science and Technology, Westminster, London SW1A 0AA.
02072192840 **@POST_UK** **post@parliament.uk** **parliament.uk/post**

risk of abuse or neglect.[31,32] More broadly, opportunities associated with sharing public sector data include:[4,33–35]

- improving quality and efficiency of public services provided by the public, private, and third sector
- ensuring external research (such as by universities or charities) can better inform policymaking and design of public services
- driving research and development innovation (such as developing smart city technologies using transport data).

Since the 2000s, public sector data have increasingly been made available for research purposes. This is partly due to greater understanding of the benefits, as well as technical advances that facilitate secure data access.[19,36] Examples of projects that facilitate access to public sector data include:

- Information Sharing Gateway – provides an administrative framework for sharing health and social care data[37]
- Administrative Data Research UK – provides researchers with access to data about use of public services[38,39]
- data.gov.uk – a search engine for finding data published by central government, local authorities and public bodies[40].

Data linkage

Data linkage (where multiple datasets referring to the same entities are combined) can provide insights that allow for a greater understanding of societal trends. Data linkage can also improve the efficiency of data collection across government and increase data accuracy (discussed later). Insights derived from data linkage can be used to develop and target services.[4,8,9,41] For example, researchers link education data with criminal records to study the relationship between educational outcomes and rates of offence, and devise interventions.[42,43] However, in the context of public service delivery, some experts have highlighted the risk that decisions made about an individual based on linked data may be unfair:[44,45] Defend Digital Me, a UK non-profit focused on children's rights, has raised concerns around how data linkage involving data collected when a child is at school could result in them being profiled and affect decisions made about them in school and later life.[57] Issues around data linkage may be exacerbated by developments in artificial intelligence (AI), which have made it possible to link and analyse increasing volumes of data at greater speed.[12,58,59]

Box 1: The existing legal framework for data sharing

- Personal data: information that relates to an identified or (directly or indirectly) identifiable individual (data subject)
- Data processing: a broad range of operations performed on data, including collecting, analysing, and sharing.[46]

The Data Protection Act 2018 (DPA) and UK GDPR

The DPA and UK GDPR together control the collection and use of personal data. They outline six lawful bases for data processing, which include: if the data subject has given consent, there are legitimate interests, or it is necessary for carrying out a task in the public interest. The most appropriate basis depends on the data sharing purpose.[47,48]

The Digital Economy Act 2017 (DEA)

The DEA provides a framework for sharing public sector data to improve public services (including water supply) and with accredited external organisations for research or statistical purposes. The DEA requires public authorities to comply with all data protection legislation (such as the DPA and UK GDPR) and to put in place data sharing agreements.[27,49]

In September 2021 the Government published a consultation on reforming the UK's data protection regime (Box 3).[21] In the same month, it also published a draft strategy 'Data saves lives: reshaping health and social care with data' proposing legislative changes for the use of health and social care data (which are not covered by the DEA).[50]

Box 2: The National Data Strategy

In September 2020, the Government published its National Data Strategy (NDS) for consultation.[1] In May 2021, the Government published its consultation response and next steps for delivery. The strategy is built around four pillars:

- **Data foundations**: improve the quality of data such that it is fit-for-purpose, findable, accessible, and interoperable
- **Data skills**: deliver data-related training through the education system and across the life course
- **Data availability**: encourage better coordination, access to and sharing of data between organisations
- **Responsible data**: ensure data use and sharing is lawful, secure, fair, ethical, sustainable, and accountable.

While the NDS has been broadly welcomed, some policy experts and stakeholders have commented that previous strategies have not achieved similar data-related goals, namely the 2010 National Information Infrastructure plan[51] and the 2017 Government Transformation Strategy.[52,16,53–56]

Risks

There are multiple risks associated with associated with sharing public sector data including those related to security, individuals' privacy, data bias, and data misuse.[13–15,60–65] Privacy and human rights experts have expressed concerns that data collection involving both private and public sector bodies can lead to increased surveillance of citizens.[64] Public concerns around government surveillance can decrease engagement with public services. In 2018, Public Health England and the British Medical Association highlighted that data sharing between government departments for immigration tracing purposes could deter people from seeking medical treatment, thus creating health risks.[66,67] Some experts have said that surveillance activities pose a further risk to civil liberties if governments use information to exert greater control over individuals' participation in society.[64,68–71] A commonly cited example is China's social credit score system.[72,73] Broader public concerns exist around private companies having greater access to personal data because of how it may be used to target and influence citizens, for example, through social media.[74–76]

Barriers

There are numerous barriers to the effective sharing of public sector data, including poor data quality and management, skills and cultural barriers, and public attitudes.[13–17] A key public concern is the trustworthiness of public sector data sharing practices.[77] A 2017 survey of 1071 UK adults by Deloitte found that 44% of respondents did not trust government organisations with their personal data. The main reasons for this were that people felt government organisations: did not have control over their data; are not good at keeping data safe and secure and; do not have individuals' best interests at heart.[78] Other surveys have found that reported trust in public bodies to handle personal data decreases when 'data sharing' is mentioned, as opposed to 'collecting and storing data',

particularly if there is a perception that data are shared for profit.[79,80] Low public trust can be partly attributed to concerns about past data breaches in the public sector and data misuses in the private sector.[10,15,79]

Requirements for effective data sharing

Legal framework

A robust legal framework for sharing public sector data can protect the rights and interests of individuals and wider society. Legal provisions and restrictions for sharing public sector data are given in the DPA, UK GDPR, and DEA (Box 1). There are different lawful bases for sharing data; for example, personal data shared under the DEA for research must be de-identified. The Information Commissioner's Office (ICO) is responsible for regulating data sharing and providing guidance.[81,82] Some sectors and local authorities provide specific data sharing advice.[83,84] There is some variation in data sharing frameworks across the four UK nations, in devolved policy areas.[53,85] In September 2021, the Government published a consultation on reforming the UK's data protection regime (Box 3).

Contractual data sharing agreements can be drawn up between organisations to outline the purpose of data sharing.[18] Data sharing agreements are widely used by public sector bodies and are required when data are shared under the DEA. Certain public bodies may enter into a memorandum of understanding with each other that fulfils the role of a data sharing agreement.[86] In some cases, licences may be used to define the terms and any fees for access to public sector data.[8]

Data management and quality

Data management and quality are key 'foundations' of data sharing.[1] Interoperability issues occur when datasets or data management systems are incompatible, and can prevent effective data sharing. These issues can arise due to limited adoption of common data standards and because large amounts of data are stored in out-dated 'legacy' IT systems that do not facilitate data sharing.[33,87,88] Poor data management can expose public sector bodies to breaches.[13–15] Security risks may be heightened when data are shared externally.[89,90]

The outcomes of sharing data depend on data quality.[7,8,91] Poor quality data may contain inaccurate, out-of-date, or incomplete information.[8,92,93] When poor quality data are analysed, the results may be inaccurate or biased.[94] For example, if data about an individual's income are incorrect then they might be unable to access benefits that they are entitled to.[95] If data about a demographic or region are missing, then policies may be developed that are not inclusive.[96–98] Data have the potential to contain historic discrimination, leading to the risk that decisions or policies informed by such data reproduce patterns of discrimination.[12,60–63,99,100] More on bias in data analyses can be found in POSTnote 633.[101] Bias may be addressed through inclusive data collection practices and diverse public participation in decisions about data processing.[59,62]

Public bodies typically focus on improving users' experience of digital services (such as by redesigning websites) rather than on more costly improvements to data foundations.[102,103] In its NDS (Box 2), the Government said that it will improve its own data foundations through a range of initiatives, including establishing a data quality framework[92] and a data standards authority.[104] Data intermediaries (see below) can improve data foundations by providing infrastructure for sharing data and replacing legacy systems.[21,105] Mechanisms for evaluating data quality, data management and organisational factors can also assist organisations in improving in these areas.[106,107]

Data intermediaries

There has been an increasing emphasis on the role of data intermediaries in supporting organisations or individuals to find, access, share, and control data. Data intermediaries broadly refer to organisations or activities that facilitate data sharing by providing forms of legal and/or technical expertise and/or infrastructure.[105,108] The key types of data intermediaries identified by the UK Government are:[47,105,109]

- **data trusts** make decisions about data (including granting data access) on behalf of individuals or organisations (this model differs to that of legal trusts)[110]
- **data exchanges** are online platforms where data can be made available to and accessed by certain users
- **personal info management systems** are platforms or tools that give data subjects more control over their data
- **industrial data platforms** provide shared infrastructure for secure data sharing and analysis between organisations
- **data custodians** provide and enable privacy-protecting analysis or checks of confidential data
- **data cooperatives** allow data subjects to establish, contribute to, and make decisions about shared datasets.

Some UK public sector bodies have trialled data intermediaries. For example, the Open Data Institute worked with the Greater London Authority to pilot a data intermediary to collect and share data about electric vehicle parking spaces.[111] However, there is scope for wider adoption of data intermediaries to improve the effectiveness and trustworthiness of public sector data sharing.[21,105,108,112]

Organisational culture and data skills

The culture within an organisation is important for data sharing and may pose a barrier. This can be due to data protection concerns or a lack of trust in data sharing mechanisms.[4,11] The risk of breaching regulatory requirements is often perceived to outweigh the potential benefits.[10,11,16,88] There may also be a lack of awareness of the benefits or confusion about the legislation and technical mechanisms for data sharing.[88] In its NDS (Box 2), the Government re-committed to tackling the culture of risk aversion around data use and sharing. Certification schemes for data processors have been proposed to increase confidence in data sharing.[21,113] Data intermediaries may also reduce cultural barriers by providing assurance or supporting public sector bodies in establishing data sharing agreements.[21,114] Provision of more specific guidance on navigating data sharing legislation has been proposed to reduce barriers to data sharing and to reduce the likelihood of data breaches.[1,94] Some experts have highlighted that a large number of people may be involved in establishing a data sharing agreement; consolidating responsibility could reduce the administrative burden on public bodies and increase compliance.[10] Forums for sharing best practice can also improve data sharing and minimise duplication of effort.[1,115,116]

Box 3. Reforming the UK's data protection regime

In September 2021, the Government published a consultation on reforming the UK's data protection regime. Proposed reforms relevant to the public sector include:[21]

- clarifying the lawful bases for sharing data, for example, by creating a limited, exhaustive list of circumstances where data can be processed under legitimate interest
- removing existing requirements for organisations to designate a data protection officer and keep a record of all data processing activities
- removing requirements for organisations to complete data protection impact assessments and consult the ICO for data processing likely to result in a high risk to individuals
- allowing businesses to share data for the purpose of improving public service delivery, as public sector authorities are empowered to in the DEA (Box 1).
- allowing a private sector body to process personal data on behalf of a public sector body without establishing a lawful ground to do so, as long as the public sector body has already established a lawful ground for processing
- introducing compulsory transparency reporting on the use of algorithms in decision-making for public sector bodies and government contractors using public data
- facilitating public-private sector data sharing to support, in particular, joint operational activity between law enforcement and national security partners.

Reception

The Open Data Institute (ODI) and others have welcomed proposals to clarify legislation but have disagreed with proposed removals from the legislation.[117] Civil rights groups and privacy campaigners have raised concerns that the proposals would reduce safeguards around the use of data and relieve organisations from considering potential harms caused by their data practices.[118,119] Other stakeholders are concerned that reformation may risk the UK's ability to freely transfer data to the European Economic Area, which would impact trade and national security.[120–126] Experts have said that barriers to sharing public sector data can and should be reduced through guidance and transparency.[16,54,94,127–129] The consultation closed in November 2021 and a response from the Government is expected in 2022.

Data skills in the public sector are essential to improving data foundations and organisational culture; this includes basic, technical, and broader skills.[1,130] Many experts have highlighted that training and upskilling (POSTnote 659) can address the lack of data skills in the public sector.[1,16,93,131] In its NDS (Box 2), the Government said it will deliver foundational and advanced data skills across the education system and improve public sector data leadership. Some groups have recommended developing data science as a profession, which would include establishing accredited training and standards.[132,133]

Privacy and consent

It is widely agreed that sharing public sector data must be done in a way that protects individuals' right to privacy.[58,60,81] Privacy is complex to define,[15,134,135] but generally, an individual has privacy when they have control over access to their private information.[13,60] This may include an individual giving consent for their personal data to be shared. However, genuine consent can be difficult to obtain because people may not read or understand information about how their data will be processed.[60,136,137] Conversely, if information is simplified, then important details may not be conveyed.[60] Consent is not often used as a lawful basis for processing public sector data (another lawful basis is usually applied, Box 1).[88] However, when consent is used, it can be challenging for public bodies to navigate: In 2015, the Royal Free London NHS Foundation Trust shared medical data relating to around 1.6 million patients with AI research company DeepMind to develop a medical app. The Trust had consent from patients to use the data for their direct benefit. However, an ICO investigation found that the consent did not extend to this case because there was no guarantee that the app would directly benefit patients.[58,138] Experts have said that the incident highlighted the wider issue of public bodies not making secure, compliant, and financially beneficial data sharing agreements with the private sector.[57,58,139]

Data cooperatives and trusts can empower individuals and organisations to control how their data is shared, allowing them to give meaningful consent.[140–142] Requiring data subjects to 'opt-in' rather than 'opt-out' of public sector data sharing is suggested to increase the meaningfulness of consent.[143,144] Privacy-enhancing technologies (PETs) can mitigate the risk of privacy breaches, for example by using advanced methods of data encryption.[145] PETs can be embedded in public sector IT systems or data intermediaries.[9,108,146] However, statistical methods, such as AI, are making it increasingly possible to use data linkage to identify data subjects in de-identified datasets.[58,147–149] Secure data access points that facilitate data analysis without revealing whole datasets can mitigate against this risk. However, many experts note that it is difficult to predict and mitigate against future motivations or technologies that could violate privacy.[13,60,79,150] Some privacy experts say that collection and sharing of public sector data, particularly personal data, should be minimised, not increased.[64,118,151]

Transparency and cooperation

The UK GDPR requires personal data to be processed in a transparent manner and specifies that certain information must be provided to an individual when their data is collected, including the lawful basis for and purposes of collection.[91] Experts agree that being clear, open, and honest with individuals about how, why, and with whom their data is shared is essential for building trustworthy public sector data sharing practices. Suggested ways to boost transparency include publishing data sharing agreements and increasing public engagement.[10,36,152,153] There are some criticisms that public engagement led by the public sector is currently too focused on one-way communication and consultation, rather than two-way dialogue.[15,36,88,93] Experts say that data intermediaries can enhance transparency and public participation.[88,134,146,154]

International data sharing may be improved through adoption of common data standards and data sharing frameworks.[9,155] The draft EU Data Governance Act aims to make more data available and facilitate data sharing across sectors and EU countries.[156] In October 2021, the G7 Trade Ministers agreed Digital Trade Principles that included aims to enable the free and trustworthy flow of data across borders by exploring common regulatory approaches and promoting interoperability.[157] Experts have said that the UK has an opportunity to lead by example and set a precedent for high data sharing standards globally.[94,155,158,159]

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Bluebell Drummond for researching this briefing, to EPSRC for funding her parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Lorna Christie.

Endnotes

1. DCMS (2020). National Data Strategy.
2. Ada Lovelace Institute (2020). The data will see you now.
3. UK Statistics Authority (2020). Statistics for the public good.
4. Administrative Data Research (2020). Applying behavioural insights to cross-government data sharing.
5. OS (2021). *Annual Report 2020-2021*.
6. Met Office (2020). Weather data for business.
7. Geospatial Commission (2020). Unlocking the power of location: The UK's geospatial strategy.
8. Coyle, D. *et al.* (2020). The Value of Data. ODI & Bennett Institute for Public Policy.
9. Borchert, I. *et al.* (2021). Addressing Impediments to Digital Trade. CEPR Press.
10. Timmis, S. *et al.* (2018). Sharing the benefits: How to use data effectively in the public sector. Reform.
11. DCMS (2020). Increasing access to data across the economy. *Frontier Economics*,
12. Royal Society (2017). Machine Learning: the power and promise of computers that learn by example, published today.
13. Véliz, C. (2020). Data, Privacy, and the Individual. Center for the Governance of Change.
14. House of Lords Select Committee on Democracy and Digital Technologies (2020). Digital Technology and the Resurrection of Trust.
15. Mac Manus, S. (2021). Dialogues about Data: Building trust and unlocking the value of citizens' health and care data. Nesta.
16. ODI (2020). Getting data right: perspectives on the UK National Data Strategy 2020.
17. Jones, K. H. *et al.* (2019). The Good, the Bad, the Clunky: Addressing Challenges in Using Administrative Data for Research. *IJPDS*, Vol 4,
18. Delacroix, S. *et al.* (2020). Democratising the Digital Revolution: The Role of Data Governance. *SSRN Electronic Journal*,
19. Ritchie, F. (2021). Microdata access and privacy: What have we learned over twenty years? *JPC*, Vol 11,
20. Harrison, T. (2020). Putting the Trust in Trusted Research Environments. Understanding Patient Data.
21. DCMS (2021). Data: a new direction.
22. ICO (2021). Response to DCMS consultation "Data: a new direction".
23. ODI (2021). Outline of the ODI's draft response to the UK data protection consultation.
24. Symons, T. (2016). Wise Council. Insights from the cutting edge of data-driven local government. Nesta.
25. National Infrastructure Commission (2018). Data for the public good DD.
26. Butler, O. (2018). Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide. *European Public Law*, Vol 24, 555–572.
27. ICO (2021). Data sharing across the public sector: the Digital Economy Act codes.
28. Deloitte (2017). Assessing the value of TfL's open data and digital partnerships.
29. HM Treasury (2018). Getting smart about intellectual property and other intangibles in the public sector: Budget 2018.
30. Deloitte (2013). Market assessment of public sector information. BEIS.
31. DHSC (2013). Child protection: information sharing project. *GOV.UK*.
32. NHS Digital (2021). Child Protection - Information Sharing project.
33. Fetzer, M. *et al.* (2021). Digital public services: what's next? Reform.
34. Dupont, J. (2018). The Smart State. Redesigning government in the era of intelligent services. Policy Exchange.
35. Social Finance (2021). Data + Digital Labs.
36. Administrative Data Research UK (2020). Trust, Security and Public Interest: Striking the Balance.
37. Information Sharing Gateway (2021). About.
38. Administrative Data Research UK (2021). https://www.adruk.org/.
39. ONS (2020). Accessing secure research data as an accredited researcher.
40. data.gov.uk (2021). Find open data.
41. Learning and Work Institute (2021). Using Labour Market Data to Support Adults to Plan for their Future Career.
42. Government Analysis Function (2021). Joined up data in government: the future of data linking methods.
43. DfE (2021). Graduate outcomes (LEO): Provider level data.
44. Chen, J. (2018). The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle. *European Data Protection Law Review*, Vol 4, 36–52.
45. Ramirez, E. (2013). The Privacy Challenges of Big Data: A View From the Lifeguard's Chair.
46. ICO (2020). Definitions.
47. (2018). Data Protection Act and The UK GDPR.
48. ICO Lawful basis for processing.
49. (2017). Digital Economy Act.
50. DHSC *et al.* (2021). Data saves lives: reshaping health and social care with data (draft).
51. Cabinet Office (2013). National Information Infrastructure.
52. Cabinet Office (2017). Government Transformation Strategy.
53. ODI (2021). Mapping data in the UK government.
54. Ada Lovelace Institute (2021). Taking back control of data: scrutinising the UK's plans to reform the GDPR.
55. Zuhlke (2020). Response to the National Data Strategy.
56. National Audit Office (2021). The challenges in implementing digital change.
57. Defend Digital Me (2020). The State of Data 2020.
58. House of Lords Select Committee on Artificial Intelligence (2018). AI in the UK: ready, willing and able?
59. Centre for Data Ethics and Innovation (2020). Review into bias in algorithmic decision-making.
60. Royal Society (2017). Data Management and Use: Governance in the 21st century.
61. Ahamat, G. (2020). Public Sector Equality Duty and bias in algorithms. Centre for Data Ethics and Innovation.
62. Patel, R. *et al.* (2021). How does structural racism impact on data and AI? Ada Lovelace Institute.
63. Turner Lee, N. *et al.* (2019). Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms. Brookings.
64. Véliz, C. (2020). *Privacy is power: why and how you should take back control of your data*. Bantam Press.
65. Seltzer, W. *et al.* (2001). The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses. *Social Research*, Vol 68, 481–513.
66. House of Commons Health Committee (2018). Memorandum of understanding on data-sharing between NHS Digital and the Home Office.
67. Chisholm, J. (2018). Guest blog: Why the MoU is not in the public's interest - BMA's views. Understanding Patient Data.
68. Zuboff, S. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile books.
69. Clavell, G. G. (2017). Protect rights at automated borders. *Nature*, Vol 543, 34–36.
70. Amnesty International UK (2020). Why we're taking the UK government to court over mass spying.

71. Toh, A. (2020). Dutch Ruling a Victory for Rights of the Poor. Human Rights Watch.
72. Liang, F. *et al.* (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure: China's Social Credit System as State Surveillance. *Policy & Internet*, Vol 10, 415–453.
73. Mistreanu, S. (2018). Life Inside China's Social Credit Laboratory. *Foreign Policy*.
74. The Royal Society (2022). The online information environment.
75. Arguedas, A. R. *et al.* (2022). Echo Chambers, Filter Bubbles, and Polarisation: a Literature Review.
76. Röttger, P. *et al.* (2020). The Information Environment and its Effects on Individuals and Groups.
77. Law Commission (2015). Data Sharing between Public Bodies: A Scoping Report.
78. Deloitte *et al.* (2017). Citizens, Government and Business. The State of the State 2017-18.
79. Davidson, S. *et al.* (2013). Public acceptability of data sharing between the public, private and third sectors for research purposes.
80. Oswald, M. (2014). Share and share alike? An examination of trust, anonymisation and data sharing with particular reference to an exploratory research project investigating attitudes to sharing personal data with the public sector. *SCRIPTed*, Vol 11,
81. ICO (2021). Data sharing: a code of practice.
82. ICO (2021). Data sharing information hub.
83. Greater London Authority (2021). Emerging Technology Charter for London.
84. The National Data Guardian for Health and Social Care (2021). Annual report 2020-2021.
85. Ritchie, F. *et al.* (2016). Five Safes: designing data access for research. Unpublished.
86. ICO Data sharing agreements.
87. National Audit Office (2019). Challenges in using data across government.
88. Centre for Data Ethics and Innovation (2020). Addressing trust in public sector data use.
89. Gharfur, S. *et al.* (2019). Improving Cyber Security in the NHS. Imperial College London.
90. ICO (2021). Guidance on AI and data protection.
91. ICO (2021). Guide to the UK General Data Protection Regulation (UK GDPR).
92. Government Data Quality Hub (2020). The Government Data Quality Framework.
93. Allsopp, R. *et al.* (2021). Data-Driven Responses to COVID-19 Lessons Learned. OMDDAC.
94. Administrative Data Research UK (2020). ADR UK Response to National Data Strategy Consultation.
95. Toh, A. (2019). The disastrous roll-out of the UK's digital welfare system is harming those most in need. Human Rights Watch.
96. UK Statistics Authority (2021). Ethical considerations in the use of geospatial data for research and statistics.
97. ONS (2021). Leaving no one behind. How can we be more inclusive in our data?
98. ODI (2021). Inclusive data: perspectives from a roundtable discussion.
99. Eubanks, V. (2017). *Automating inequality: how high-tech tools profile, police, and punish the poor*. St. Martin's Press.
100. Obermeyer, Z. *et al.* (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, Vol 366, 447–453. American Association for the Advancement of Science.
101. Molnar, C. (2020). Interpretable Machine Learning.
102. White, C. (2019). A platform-first approach. *LocalGov*.
103. Local Government Association (2014). Transforming local public services.
104. Marshall, R. (2020). Introducing the Government Data Standards Authority. GOV.UK.
105. Centre for Data Ethics and Innovation (2021). Unlocking the value of data: Exploring the role of data intermediaries.
106. Royal Society DELVE Initiative (2020). Data Readiness: Lessons from an Emergency.
107. GOV.UK (2021). Data maturity model: user needs.
108. Ada Lovelace Institute (2021). Exploring legal mechanisms for data stewardship.
109. ODI (2019). Data trusts: lessons from three pilots.
110. Pinsent Masons *et al.* (2019). Data trusts: legal and governance considerations.
111. ODI (2019). Greater London Authority and Royal Borough of Greenwich Data Trust Pilot.
112. DCMS (2021). National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy.
113. Snaith, B. *et al.* (2021). Assurance, trust, confidence – what does it all mean for data? *ODI*.
114. Snaith, B. *et al.* (2021). How does data assurance increase confidence in data? *ODI*.
115. Connected Health Cities (2020). Hub.
116. London Office of Technology & Innovation (2021). 35 guides, toolkits and templates developed by the LOTI community.
117. ODI (2021). Data: a new direction. Open Data Institute response.
118. Delli Santi, M. (2021). ORG response to Data: a new direction. Open Rights Group.
119. Open Rights Group *et al.* (2021). Data Reform Consultation Roundtable Focussing on the Privacy and Digital Rights of Individuals.
120. Data & Marketing Association (2021). Data: A New Direction – Roundtable Summary.
121. Preiskel & co (2021). UK National Data Strategy: a step further away from an adequacy decision under the GDPR?
122. O'Neill, M. *et al.* (2021). UK Government's Consultation – Data: A New Direction. *Thorntons*.
123. Powell, E. (2021). A new direction in Data Protection. *Hugh James*.
124. Long, W. R. *et al.* (2021). Data: A New Direction or Misdirection? ICO Responds to UK Government Consultation on Its Proposed New Data Protection Regime. *Sidley*.
125. ODI *et al.* (2021). UK data protection changes: impact on research.
126. Bird, A. (2021). Back to EU.
127. ICO (2020). The ICO's response to the DCMS consultation on the National Data Strategy.
128. Delli Santi, M. (2021). Why on earth is the Government mucking about with our privacy laws? *Open Rights Group*.
129. ODI (2021). Roundtable summary note: data sharing for public services.
130. ODI (2020). Data Skills Framework.
131. Allsopp, R. (2021). Data-driven public policy. OMDDAC.
132. Royal Society (2019). Dynamics of data science skills. Royal Society.
133. British Computer Society (2021). Alliance formed to create new professional standards for data science.
134. Ada Lovelace Insitute (2021). Participatory data stewardship.
135. Royal Society *et al.* (2020). Engagement as a mode of operation.
136. Solove, D. J. (2012). Introduction: Privacy Self-Management and the Consent Dilemma Symposium: Privacy and Technology. *Harv. L. Rev.*, Vol 126, 1880–1903.
137. Cohen, J. E. (2012). What Privacy is For Symposium: Privacy and Technology. *Harv. L. Rev.*, Vol 126, 1904–1933.
138. ICO (2017). Royal Free - Google DeepMind trial failed to comply with data protection law.

139.Dixon, R. *et al.* (2019). Should councils collaborate? Evaluating shared administration and tax services in English local government. *Public Money & Management*, Vol 39, 26–39.
140.DataEthics (2021). A Data Democracy Comes With Individual Data Control.
141.Bunting, M. *et al.* (2019). Designing decision making processes for data trusts: lessons from three pilots. Involve.
142.Delacroix, S. *et al.* (2020). From Research Data Ethics Principles to Practice: Data Trusts as a Governance Tool. *SSRN Electronic Journal*,
143.Vezyridis, P. *et al.* (2017). Understanding the care.data conundrum: New information flows for economic growth. *Big Data & Society*, Vol 4, 205395171668849.
144.Presser, L. *et al.* (2015). Care.data and access to UK health records: patient privacy and public trust. *Technology Science*,
145.Centre for Data Ethics and Innovation (2021). Privacy Enhancing Technologies Adoption Guide.
146.ODI (2021). Data reform: strategic opportunities and the long view.
147.Horvitz, E. *et al.* (2015). Data, privacy, and the greater good. *Science*, Vol 349, 253–255.
148.Finck, M. *et al.* (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, Vol 10, 11–36.
149.Ritchie, F. *et al.* (2018). Confidentiality and linked data. *National Statistician's Quality Review into Privacy and Data Confidentiality Methods*,
150.ODI (2020). Monitoring Equality in Digital Public Services.
151.Law Commission (2015). Data Sharing between Public Bodies: A Consultation Paper.
152.Ada Lovelace Insitute (2020). Transparency mechanisms explainer for UK public-sector algorithmic decision-making systems.
153.Oswald, M. *et al.* (2021). Data Sharing in a Pandemic: Three Citizens' Juries. National Institute for Health Research.
154.National Data Guardian for Healthcare (2016). Review of Data Security, Consent and Opt-Outs.
155.Government Office for Science (2020). Evidence and scenarios for global data systems.
156.European Commission (2020). Data Governance Act.
157.Department for International Trade *et al.* (2021). G7 Trade Ministers' Digital Trade Principles. *GOV.UK*.
158.ODI (2021). Spending Review 2021: Investing in data to build back better.
159.Dove, E. S. *et al.* (2021). Raising standards for global data-sharing. *Science*, Vol 371, 133–134.