Data management and use: Governance in the 21st century

A joint report by the British Academy and the Royal Society

BRITISH ACADEMY

for the humanities and social sciences

THE ROYAL SOCIETY

Contents

The report at a glance **2**

Executive summary **4**

1 Introduction: Changing data, changing society **12**
1.1 An increasingly complex picture 15
1.2 Drivers of complexity 17
1.3 Process and context for this report 24

2 Data governance: Tensions and disconnects **26**
2.1 The case for change 27
2.3 Tensions in data management and data use 40
2.3 Strained systems of governance and the responses required 47

3 Principles for Data Governance **50**

4 Essential functions and stewardship **58**
4.1 Essential data governance functions 59
4.2 Ensuring effective stewardship through the creation of a new body 73
4.3 Options and models for stewardship 79

Annexes **82**
Annex A Governance bodies 83
Annex B Terms of reference 88
Annex C Acknowledgements 89
Annex D Evidence and engagement 92

Glossary 94

The report at a glance

Changing data, changing society

- As data collection activities continue to increase in speed, scale and variety, and the analytic techniques used to process these datasets become more sophisticated, individuals and communities are affected in new and unexpected ways.

- Meanwhile, the uses of data-enabled technologies promise further benefits, from improving healthcare and treatment discovery, to better managing critical infrastructure such as transport and energy.

- In this fast-moving landscape, governance challenges need to be addressed in a timely manner if the overall system of governance for data management and data use is to maintain public trust:

    - Existing data governance concepts, such as privacy and consent, are under unprecedented strain: their meanings in policy, law and public discourse have shifted, and will continue to do so in new and unpredictable ways.

    - Uncertainties are accumulating and compounding and acting on them is necessary, but in order to avoid long-term, cumulative and difficult-to-foresee effects any action must be carefully considered.

    - Risk of public, data-related controversy: history has provided rich illustrations of how the widespread adoption of new technologies can increase public anxiety, or result in major public controversy, both of which risk hampering potential benefits.

Principles for Data Governance

- A set of high-level principles is needed to visibly shape all forms of data governance and ensure trustworthiness and trust in the management and use of data as a whole.

- The promotion of **human flourishing** is the overarching principle that should guide the development of systems of data governance. The four principles that follow provide practical support for this overarching principle across the varied ways data is managed and used:

- protect individual and collective rights and interests
- ensure that trade-offs affected by data management and data use are made transparently, accountably and inclusively
- seek out good practices and learn from success and failure
- enhance existing democratic governance.

Essential functions and stewardship

- The governance framework for data management and data use should perform three broad categories of functions. These may be carried out by a variety of public and private actors:
  - **A**nticipate, monitor and evaluate
  - **B**uild practices and set standards
  - **C**larify, enforce and remedy

- Despite the range of actors already carrying out some of these important governance functions in their specific sectors or domains, there is a clear need **for a new body** to steward the landscape as a whole, rather than being directly responsible for implementation within specific domains.

- The purpose of such a stewardship body would be to support delivery of the full breadth of critical functions in accordance with the principles set out above.

- We expect that such a body would primarily recommend actions to others, but it may also need the capacity to carry out some functions itself if they could not be performed elsewhere, being careful to not duplicate existing efforts.

- This stewardship body would be expected to conduct inclusive dialogue and expert investigation into novel questions and issues, and to enable new ways to anticipate the future consequences of today's decisions.

- The characteristics of such a stewardship body are that it should be:
  - Independent
  - Deeply connected to diverse communities
  - Expert across and beyond disciplines
  - Tightly coupled to decision processes
  - Durable and visible
  - Nationally focused but globally relevant

Executive summary

Changing data, changing society

The amount of data generated from the world around us has reached levels that were previously unimaginable. New technologies are generating data in new ways: as wearable devices quantify individuals' health, social media sites provide platforms to share details about day-to-day life, and companies across sectors rely on data about their daily business and activities to improve their products and processes. Other data capture may happen less deliberately, as individuals walk around retail spaces equipped with sensors, connect to public Wi-Fi hotspots, or use services such as on-demand taxis.

Fascinating new forms of data analysis such as machine learning have vastly increased the ability to link this data and use the patterns that emerge. As data collection activities continue to increase in speed, scale and variety, and the analytic techniques used to process these datasets become more sophisticated, individuals and communities are affected in new and unexpected ways. Meanwhile, the uses of data-enabled technologies promise further benefits, from improving healthcare and treatment discovery, to better managing critical infrastructure such as transport and energy.

To realise these benefits, societies must navigate significant choices and dilemmas: they must consider who reaps the most benefit from capturing, analysing and acting on different types of data, and who bears the most risk; they must consider, as best they can, the implications of the future nature and distribution of work, wealth and skills; they must ensure that the personalisation of news and views does not limit the diversity and richness of public debate or even undermine those practices of checking and challenging claims that underpin democracy.

In the past, disruptive technologies, such as the printing press or the introduction of weaving machines during the first industrial revolution, sparked major public controversy. While history does not enable us to predict the future, it suggests that the potential for controversies around new ways of using and communicating data is very high. It also suggests that societies can act in advance to create well-founded responses that contribute to bringing the benefits of disruptive technologies into being. Current experience also suggests that, without a framework giving entrepreneurs and decision-makers sufficient confidence about acceptable data uses, applications that would have been widely welcomed may be lost.

Meeting the challenges of data governance in the 21st century

In this report, we consider data governance to mean everything designed to inform the extent of confidence in data management, data use and the technologies derived from it. We cannot properly consider this by treating data management or data use individually, or separately from each other. While data management and data use may previously have been separate activities, the two are now often tangled with each other, across applications and across the world. To achieve a meaningful discussion about data governance, it is therefore necessary to consider both together. Such integration requires a new approach to framing questions about data governance and, in this context, purpose is of overarching importance.[1]

The changing nature of data management and data use, the evolving technological context, and the shifting meaning of core governance concepts, place today's systems for data governance under stress. The impact of these changes is further compounded by their speed. These factors create new challenges for data governance, making a review of the governance landscape both timely and necessary. Our review of the capability of the UK governance landscape did not find an immediate failure in law. However, we are strongly of the view that, while the current governance architecture provides a great deal of what is necessary for the here and now, there are very clear gaps between today's framework and what is needed to meet the future challenges of data governance in the 21st century.

From questions such as how individual and collective benefits and risks are negotiated, to the uncertain future of ownership and the role of human agency, we have identified a range of significant tensions in the way data is managed and used. The significance of these tensions is growing and the potential implications of the ways they are accommodated are accumulating. Furthermore, given the current pace of change, the vocabulary used to discuss data management and data use is also shifting. Some of the concepts that were core to public confidence in governance during the 20th century are becoming increasingly contested. The meanings in policy, law and public discourse of notions such as accountability, agency, consent, privacy and ownership have changed, and will continue to change. In some areas society cannot yet frame meaningful questions around these issues, but nevertheless actions are being taken now that will have long-term and cumulative effects.

1 Throughout this report we use the term 'data governance' as shorthand to refer to the governance of data management and data use. In instances where the distinction between the governance of data management and the governance of data use is relevant, we aim to make that clear. In some cases, distinctions between data, content or information and the communication of these may also be relevant, and should be considered when taking forward issues outlined here.

We recognise that data governance is linked intimately to the governance of so much of life that each step is simply another in the journey, where aspiration, action, evidence, reflection and debate will all continue to play essential parts. That is part of the challenge and one of the reasons for this review.

While there are governance challenges that are general in nature, many of them – and their effects – are likely to be specific. The primacy of purpose means that most forms of governance are, and should be, specific to context. For example, the use of data to create personal recommendations for online shopping creates different forms of benefit and risk and involves different types of actors compared to the use of data in healthcare. It would be a mistake to attempt to govern them in the same way.

At the same time, new ways of using data and the interconnected nature of digital systems mean that governance frameworks and mechanisms designed for one purpose or application may have implications for its use in another. For example, transport data may inform health choices, or commercial data may be used to target public services. There is great scope for benefit here, but also great challenges arising from common underlying themes such as privacy, consent, bias and quality. As different sectors grapple with these challenges, it is likely that there is much to be learned from each other.

Taking these factors together, we believe two types of response are essential.

First, a renewed governance framework needs to ensure trustworthiness and trust in the management and use of data as a whole. This need can be met through a **set of high-level principles** that would cut across any data governance attempt, helping to ensure confidence in the whole system. As effective data governance strongly resists a one-size-fits-all approach, grounding efforts in underlying principles will provide a source of clarity and of trust across application areas. These are not principles to fix definitively in law, but to visibly sit behind all attempts at data governance across sectors, from regulation to voluntary standards.

Second, it is necessary to **create a body to steward the evolution of the governance landscape as a whole**. Such a body would not duplicate the efforts of any existing body. Rather, it would seek to ensure that the complete suite of functions essential to governance and to the application of the high-level governance principles is being carried out across the diverse set of public and private data governance actors. These functions would include activities to anticipate future challenges and to make connections between areas of data governance. Because many types of data management – or technologies making use of data – have significant or contested social values embedded within them, such a body would need strong capacities for public engagement, deliberation and debate. We see this body as an essential step in stewarding the governance landscape during the period of particularly disruptive transition that societies face in the coming years.

Recommendations

Principles for Data Governance

Drawing on insights into the application of principles in law and practice across other areas of society, we propose the introduction of four high-level principles informed by one overarching principle. These principles are intended to be simple, memorable, and provide guidance to those considering new forms of governance. The way they are applied is therefore key and should require argument, challenge and debate, as their full meaning will be determined by those debates and the actions surrounding them.

The overarching principle is that systems of data governance should promote **human flourishing**. This framing includes concepts such as wellbeing and the need for individuals and communities to thrive, but it is deliberately broad. At moments of contention, the principle should serve to reflect the fundamental tenet that society does not serve data but that data should be used to serve human communities.

Four high-level principles complement the need to promote human flourishing, by setting a framework to enable well-founded debate about the tensions inherent in data governance. These principles are that the systems of data governance should:

- **protect individual and collective rights and interests**
- **ensure that trade-offs affected by data management and data use are made transparently, accountably and inclusively**
- **seek out good practices and learn from success and failure**
- **enhance existing democratic governance.**

Functions required for a successful data governance landscape

The core functions necessary for a successful data governance landscape are those that would be required for any complex social and technological system undergoing rapid evolution. The governance system needs to:

- **A**nticipate, monitor and evaluate: considering alternative futures, managing risks, keeping pace with changes, and reflecting on performance.

- **B**uild practices and set standards: enabling and continuously improving well-founded practices that can be spread quickly across relevant sectors and uses.

- **C**larify, enforce and remedy: ensuring sufficient arrangements for evidence gathering, debate and decision-making, and for action in the forms of incentives, permissions, remedies for harm, incentives and penalties.

These functions are carried out to differing extents across the existing governance landscape by a variety of public and private actors with diverse roles. Some actors are sectoral, such as bodies related to health, while others, such as the Information Commissioner's Office, consider particular types of data across sectors. This variety reflects the complexity and range of data management and data use, and it would be impossible and also undesirable to try to centralise governance.

While these existing actors already carry out a range of important governance functions in their specific sectors or domains, we have identified a clear gap for a new stewardship body. This body would be charged with stewarding the governance landscape as a whole, rather than being directly responsible for implementation within specific domains. The purpose of this body would be to support delivery of the full breadth of critical functions wherever they are needed, in accordance with the Principles for Data Governance, but would not entail formal regulatory and enforcement power. We expect that such a stewardship body would recommend actions to others, as well as carry out some functions itself where they could not be done elsewhere. This stewardship body would be expected to conduct inclusive dialogue and expert investigation into novel questions and issues, and to enable new ways to anticipate the future consequences of today's decisions.

The core characteristics of a new stewardship body

In this report, we do not make specific recommendations about the location, funding or precise status of a new stewardship body for data governance. Instead, we apply the Principles of Data Governance alongside experience from other sectors to the stewardship body itself to derive a set of characteristics that will help ensure that it is trusted and trustworthy. We consider such a body must be:

- **independent** from industry, civil society, academia and government, to develop and maintain a reputation as a trusted voice on issues of contention and controversy
- **deeply connected to diverse communities**, to create dialogue with and between publics, industry, civil society, academia and government
- **expert across and beyond disciplines**, to draw on diverse sources of knowledge, ideas and on a wide range of practitioners to tackle the daunting unresolved questions raised by the present and future of data governance
- **tightly coupled to decision processes**, shaping agendas and implementation, and referred to formally or informally
- **durable and visible**, set up with a timeframe long enough to build the needed trust, legitimacy and visibility to maintain broad and lasting confidence
- **nationally focused but globally relevant**, to shape thinking on an international level and learn from and adapt world-leading evidence and experience.

1 Introduction: Changing data, changing society

Changes to how data is generated, collected and processed are contributing to an increasingly complex data environment. Such changes are driven and compounded by the pervasiveness of common technology, such as: the internet and mobile devices for data collection and use; the ability to derive increasingly detailed insights from data in unexpected ways; and the increasing difficulty and importance of ensuring the quality of data.

The accelerating exchange and use of data is affecting everyday lives, activities and communities in new and unexpected ways. Data-enabled technologies can stimulate innovation and efficiency in public services, provide evidence for research, improve productivity and deliver significant economic and wider social benefits to the UK. To encourage constant innovation, and to ensure public confidence and maximise benefits, the UK needs a governance framework for data management and data use that can engender authority and trust.

While the current governance architecture provides a great deal of what is necessary for the here and now, there are very clear gaps between today's framework and what is needed to meet the future challenges of data governance in the 21st century. Today's governance systems – including laws, norms and technologies – are grounded in assumptions that are at risk of becoming outdated as the use of digital technology expands.

Box 1: Governance of data management and data use

In this report we consider 'data governance' to mean everything designed to inform the extent of confidence in data management, data uses and the technologies derived from it. We start from the overarching importance of purpose. We cannot properly consider purpose by considering data management or data use individually or separately. These stages, which used to be more separate, are now often tangled with each other across applications and across the world. To meaningfully discuss data governance, there is an increasing need to integrate the governance of both.[2]

Recognising the new governance challenges posed by this changing data environment, the British Academy and the Royal Society initiated this review of data governance. The aim is to characterise and illustrate some of the changes that expanding data management and data use have brought about, the tensions arising from these changes, and the ways in which a principle-based approach to data governance can provide direction and stewardship during a potentially disruptive period of transition.

2 Throughout this report we use the term 'data governance' as shorthand to refer to the governance of data management and data use. In instances where the distinction between the governance of data management and the governance of data use is relevant, we aim to make that clear. In some cases, distinctions between data, content or information and the communication of these may also be relevant, and should be considered when taking forward issues outlined here.

Perspective 1
The concept of governance

Karen Yeung is Professor of Law and Director of the Centre for Technology, Ethics & Law in Society (TELOS) at the Dickson Poon School of Law.

Professor Yeung explains how complex global challenges are affecting the traditional levers of control by government, and suggests that the rise in popularity of the word 'governance' stems from a recognition that many different actors and institutions beyond the state are now deeply involved in managing today's challenges and risks.

While the concept of 'governance' has recently become very fashionable to discuss in public policy and study in the social sciences, it remains ambiguous and is subject to many meanings in different communities and contexts. It is frequently used instead of the term 'government' to signify some kind of change in the way that governing is now undertaken. Used in this way, governance denotes new processes of governing, changed conditions of ordered rule, or new methods by which society is governed. Academic commentators have argued that these changes represent a paradigm shift in the way modern societies are governed, suggesting that authority is (or can be) institutionalised in different spheres or arenas (each with different norms, processes and degrees of formality), and that these different institutional frameworks may interact with each other in different ways.

Some argue that the increasing complexity of modern society, rapid technological innovation and the globalisation of many commercial and other activities have generated new risks and have engendered new democratic expectations. As a result, those who seek to exert control over the activities and decisions of others are no longer able to apply effective authority through traditional approaches to control based on hierarchical chains of command that characterised the tasks of government several decades earlier. Hence, it is claimed that both national governments and other spheres of authority need to develop new modes of control, building their capacities to govern indirectly through developing and harnessing their steering capacities. Within this literature, there is widespread recognition that the state is not the only legitimate actor involved in the task of 'governing' a sphere of activity, and that sources of standard-setting, oversight and information gathering, and enforcing compliance with those standards, may properly be undertaken by multiple institutions including, but not limited to, the state itself.

The emergence and plurality of new modes and institutions involved in the task of governance have been associated with new political and policy dynamics, new understanding of institutions both of and beyond the state, and new ways for managing risks, with the potential to empower citizens and promote new and experimentalist forms of democratic decision-making.[3]

1.1 An increasingly complex picture

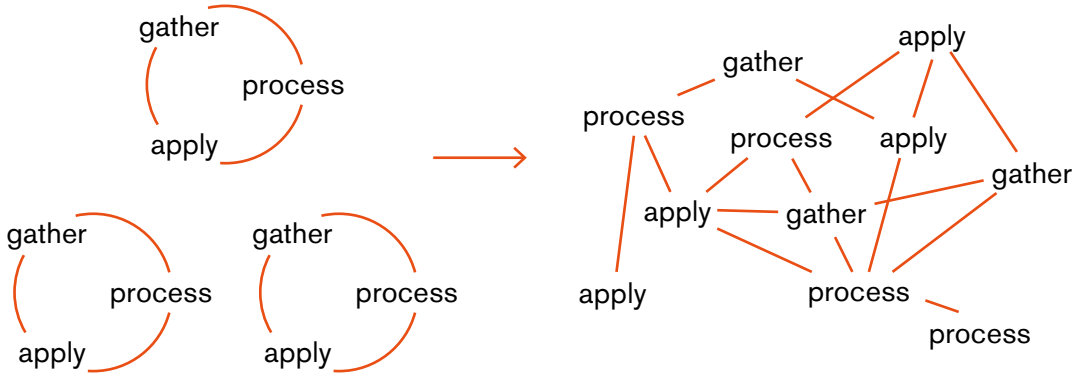
Data has always played a role in society. Long before the advent of modern digital technologies, governments, organisations and individuals have collected data, processed it, applied it to problems of social or commercial relevance, and used the insights generated to inform further collection, processing or application. This process can be thought of as a 'data lifecycle'.

The traditional data lifecycle was clear, relatively sequential, predictable, often managed by a single organisation and made it comparatively easy to erase data sets that were no longer needed. These characteristics also meant that data governance could focus on a specific point in the 'cycle', such as on collection, and use this single point to gain significant leverage over the broader process. However, this traditional approach is now under considerable strain.

The core cause of this strain is the increased complexity of data lifecycles. Instead of individual organisations operating independent data lifecycles, with linear approaches to processing, data is now generated and exchanged across many organisations, often without the subject's awareness. Each activity also creates new data for different organisations at every layer of society's infrastructure.

It is therefore no longer appropriate to think in terms of independent clear data lifecycles, but rather of interconnected and interdependent *open networks of data* (see Figure 1). In this increasingly complex network, traditional governance points of interventions and societal steer are no longer fit for purpose.

Figure 1: Open networks of data



3 Levi-Faur D. 2012 From 'Big Government' to 'Big Governance' and Rhodes RAW. 2012 Waves of Governance. In: Levi-Faur D (ed.) *The Oxford Handbook of Governance*, Oxford, UK: Oxford University Press; Rhodes RAW. 1996 The new governance: governing without government. Political Studies **44**, 652–667.

Perspective 2
Historical context of data use

Jon Agar is Professor of Science and Technology Studies at University College London, with an interest in contemporary technologies such as mobile phones and ID cards, as well as the history of modern science and technology.

Professor Agar explains how data-driven decisions are older than commonly thought, and how concerns about privacy and automation go back much longer than any data revolution. He emphasises that policymakers focus too much on governing new technologies, when it is often the older ones that really matter.

Data is increasingly important to how governments, businesses and other organisations work, and how we, as citizens or consumers, relate to them. This data rush is productive, but also overwhelming. New valuable services are created but so too are deep concerns, not least around privacy or unemployment through automation. If this is what we think is happening now, how might a historical perspective help?

First, a useful corrective: much of what we think is new is not new at all. Data – information organised for use by information technologies – has an ancient pedigree. The technologies have changed, but organisations have been co-produced with the means of managing information, from the cuneiform tablet and the Babylonian state, through to the filing systems of the Victorian bureaucracy to the electronic communications tools of today.[4] Between 1550 and 1750, Europeans experienced an 'information explosion', during which they complained of feeling overwhelmed by data.[5]

Second, while threats, such as those to secure employment or privacy, are often cast as being caused by technological change, history shows that the relationship between social and technological change is much more subtle. Our current governance framework for data privacy emerged between the 1960s and 1980s. But the sharp rise of concerns about privacy began well *before* they became associated with computer surveillance. Any connection was a contingent one. There was nothing historically inevitable about how we came to think about technology and privacy. Likewise, there have been recurrent anxieties about automation, roughly on a 20-year cycle. But each time a historian has dug into the full story, they have

4 Hobart ME and Schiffman ZS. 1998 *Information Ages: Literacy, Numeracy, and the Computer Revolution*. Baltimore: Johns Hopkins University Press; Agar J. 2003 *The Government Machine: a Revolutionary History of the Computer*. Cambridge, MA: MIT Press.

5 Rosenberg D. 2003 Early modern information overload, *Journal of the History of Ideas*. **64**, 1–9.

shown that it was never a simple case of technological impact. The 1950s' panic about automation, for example, was more about cold war paranoia than the innovation of new Soviet automated factories. The 1820s' claims about automation in industry were more about eliding the human worker (and his or her agency) than they were a factual description of industrialisation.[6]

Historians can point to past patterns that, as generalisations backed by documentary evidence, should be held in view when we think about governance of technology. Technologies are shaped by users just as much as by designers, inventors or regulators.[7] Moreover these patterns of use can be unexpected or unanticipated. Old technologies (including information technologies) continue to be as important, or even more important, than the novel technologies that attract the attention of policymakers.[8] When thinking about the governance of data, we should bear in mind the likelihood of unexpected users and uses, as well as the continuing centrality of older ways of storing and processing data. Finally, technologies embed social values, because they are shaped powerfully by social interests,[9] and therefore these values need to be discussed using all the deliberative tools of democracy for them to reflect the public good.

1.2 Drivers of complexity

Four key trends are contributing to the increasingly complex data environment.

- **Data capture and processing is increasingly pervasive**: More data is being collected or generated, at new scales and by new actors. Huge amounts of data are now produced on a daily basis: some of this is linked to new societal uses of technology, as wearable devices quantify individuals' health, social media platforms record the minutiae of daily life, and companies across sectors produce data to improve their products and processes. Other data capture happens less deliberately, as individuals walk around retail spaces equipped with sensors, connect to public Wi-Fi hotspots, or use services such as on-demand taxis.

6 Schaffer S. 1994 Babbage's Intelligence: Calculating Engines and the Factory System, *Critical Inquiry*. **21**, 203–227.

7 Pinch T and Oudshoorn N. 2003 *How Users Matter: The Co-Construction of Users and Technology*. Cambridge, MA: MIT Press.

8 Edgerton D. 2006 *Shock of the Old: Technology and Global History since 1900*. London: Profile.

9 MacKenzie D. 1996 *Knowing Machines: Essays on Technical Change*. Cambridge, MA: MIT Press; Winner L. 1986 *The Whale and the Reactor*. Chicago: University of Chicago Press.

There is relatively little public awareness of what data is collected and used.[10] This applies in particular to passive methods of data collection such as social networking sites collecting information from personal posts.[11] Research undertaken by Ipsos MORI for the Royal Society[12] similarly demonstrated low awareness of the potential uses of large datasets.

- **Data collection and use are becoming harder to separate**: Whereas previously data would be collected about a specific activity in order to inform a specific purpose, the link between data collection and pre-defined purpose is weakening. The ease of collecting and managing large volumes of data in 'big data' platforms and the availability of new tools to analyse such data – such as machine learning[13] – means that large volumes of data can be collected, integrated and analysed in ways that generate unexpected patterns or insights which go far beyond the original intended purpose of data collection.

  For example: energy data from smart meters can contain information about lifestyle, such as which television channels people watch, whether they set a burglar alarm, and how often they come home at pub closing time;[14] and mobile phone mast data can contain information about how individuals move, which can be used to infer where they live, what they do, and their socio-economic status.[15]

10 The British Academy and Royal Society. 2017 *Public Engagement Literature Review*, 2017, 'Awareness' section.

11 Ipsos MORI (report prepared for the Wellcome Trust). 2016 The One-Way Mirror: Public attitudes to commercial access to health data. See https://wellcome.ac.uk/sites/default/files/public-attitudes-to-commercial-access-to-health-data-wellcome-mar16.pdf (accessed 22 December 2016).

12 Ipsos MORI (research conducted for the Royal Society). 2017 *Public views of machine learning: findings from public research and engagement*.

13 The Royal Society. 2017 *Machine learning: the power and promise of machines that learn by example*. London: The Royal Society. See https://royalsociety.org/topics-policy/projects/machine-learning/ (accessed 10 June 2017).

14 Brown I. 2014 Britain's smart meter programme: A case study in privacy by design. *International Review of Law, Computers & Technology*. **28**, 2 and Data Governance: Case Studies (2017). See http://dx.doi.org/doi:10.1080/13600869.2013.801580 (accessed 10 June 2017).

15 Smith-Clarke C, Mashhadi A, Capra L. 2014 Poverty on the cheap: Estimating poverty maps using aggregated mobile communication networks. In: *CHI '14: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. See http://dx.doi.org/doi:10.1145/2556288.2557358 (accessed 10 June 2017).


Managing money
Mobile banking, using credit or debit cards, and loyalty cards create information about shopping habits
At work
Email systems and remote access networks, photocopiers, and other machinery can collect usage data
Using public services
Accessing public services creates records relating to pensions, policing, healthcare, tax, and more
Everyday activities generate a huge amount of data
On the move
Contactless travel cards, sensors on cars, and mobile devices can collect location information
In the home
Internet browsing, TV streaming, and energy usage create data at home

Because data can contain unexpected but valuable insights, it is not always captured to serve a specific analytic purpose, and is often accumulated from multiple sources as a by-product of some other exercise. For example: recording credit card transactions to calculate a credit card bill; health data from health trackers intended to record the number of steps an individual has taken;[16] or data about sub-optimal agricultural practices or areas of poverty from satellite data.[17]

As the potential benefits of these new applications are revealed, there are increasing incentives for data to be linked across sectors and applications. This fuels a shift of data collection efforts to focus on curating and processing continuous and distinct data streams from many different sources.

Managed effectively, the insight from such advanced analytics can offer substantial benefits, such as improved public service delivery.[18] But it can also increase the risk of potential harm to individuals and communities.

16 In data protection law, 'purpose limitation' attempts to limit repurposing, although in practice significant repurposing is common. For the legal aspects of legitimate interest arguments in data protection, see British Academy and the Royal Society. 2017 *Data Governance: Landscape Review.*

17 The Royal Society. 2016 *From satellite to soil: connecting environmental observation to agri-tech innovations: conference report.* See https://royalsociety.org/~/media/events/2016/06/obs-and-agritech/DES4502_TOF_Environmental%20Observation%20conference%20report%20WEBCOPY.pdf?la=en-GB (accessed 10 June 2017).

18 For example, the Digital Bill, which received Royal Assent in April 2017, has provisions to better identify and target individuals living in fuel poverty. However, the Bill has also been criticised for lacking clarity on data sharing. See British Academy and the Royal Society. 2017 *Data Governance: Landscape Review.* London: The Royal Society.

Box 2: Data protection

In the UK, other European countries, and some other jurisdictions such as Canada and Australia, data protection legislation has been the main approach to trying to manage challenges associated with personally identifiable data. Data protection law emerged from pressures to govern privacy in the face of computational processing at national level, (Germany was an early key player), and international level, through the Organisation for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

In the UK, the most relevant data protection law will be the General Data Protection Regulation (GDPR) that will come into force from 25 May 2018 and replace the current Data Protection Act 1998. It notably applies only to personal data, defined in terms of that person's identifiability on the basis of that data. Where data is non-personal, or sufficiently de-personalised[19] from an individual, it ceases to fall under the scope of data protection law.

Yet as discussed above, for practical purposes, sufficient anonymisation is becoming less achievable as society becomes more connected. Consequently it is becoming less clear as to whether specific categories of data are sensitive. Rather, what may be sensitive is the use of data. The Information Commissioner's Office generally recognises this contextual approach and focuses on the risk to the individual in the round, rather than only on the nature of the data involved. However, data protection law, which is still framed in a simple binary system[20] will have to cover increasingly broader categories of data than originally envisaged.[21]

The Data Governance: Landscape Review[22] discusses a range of other uncertainties around the GDPR.

19 The term 'de-personalised' is the term suggested by the Understanding Patient Data initiative to refer to what is known as de-identified data. The initiative was set up following the Caldicott Review to facilitate public debate about anonymised data. See: Understanding Patient Data. n.d. Identifiability Demystified. See https://understandingpatientdata.org.uk/sites/default/files/2017-04/Identifiability%20briefing%205%20April.pdf (accessed 10 June 2017).

20 For a discussion on attempts to address these challenges in the GDPR, please see British Academy and The Royal Society. 2017 *Data Governance: Landscape Review*, p. 29–30.

21 Butler D. 2007 Data sharing threatens privacy. *Nature* 449(7163): 644–645.

22 In particular, see British Academy and The Royal Society. 2017 *Data Governance: Landscape Review*, Section 3.4.

- **Non-sensitive data can hold sensitive insights**: In an environment where data insights can no longer be predicted at the point of collection, it is difficult – or near impossible – to be certain whether data initially considered non-sensitive might subsequently reveal sensitive information as a result of linking with new datasets or exposure to new analytic techniques.[23] Existing forms of data that people have readily shared online, such as videos, images or text, now betray considerably more information than when existing governance mechanisms were shaped. Robust and future-proof anonymisation is becoming increasingly challenging as the data environment becomes an interlinked and open network.

  The global nature of data, where it travels easily across borders and jurisdictions, adds an additional dimension to this challenge. Once sensitive data is available in the public domain it becomes extremely difficult to thoroughly recall.

- **It is becoming more challenging to know where data comes from**: As data is transmitted to new contexts, the assumptions used when the data was gathered may no longer be appropriate for this new use.[24] Data is also subject to errors and degradation. Data values that were valid in the past may not be correct now.

  Data about data – such as the context, meanings, formats, validation parameters and collection date – is referred to as its metadata. To be robust, as data sets are copied to new systems and organisations, this metadata needs to accompany it. Metadata provides an audit trail, just like the provenance information that must accompany a rare painting for its authenticity to be verified.

  Access to metadata is crucial to being able to make quality assessments when data is being used to make and support important decisions. Yet, as data sets are copied, transferred and transformed, it is not straightforward how to develop verifiable and agreed ways to track metadata and lineage.

  Knowing in advance which data sets are of poor quality or misrepresentative is far from simple. This was arguably a simpler calculation to make when the logic of data collection and its use were more tightly coupled. As data streams are purposed and repurposed, the reliable and useful signals of provenance become more important yet harder to achieve.

23 Kosinski, M, Stillwell D, and Graepel T. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences* 110.15 (2013): 5802–5805.

24 For example, the Administrative Data Research Centre England (ADRCE) notes that, while administrative data has the benefits of relatively low cost, large sample size, comprehensive coverage, and their direct relationship to services (and hence relevance for policy and practice), the disadvantages include variation in data quality and the fact that the data measures events or characteristics captured by the service, rather than actual events or characteristics experienced by the individual. See British Academy and The Royal Society. 2016 *Data Governance: Call for Evidence*.

Furthermore, as data is used to train algorithms and insights from data become embodied in algorithms that are traded, knowing where data comes from is likely to become significantly more difficult.

Perspective 3
A short history of the census

Edward Higgs is a Professor in History at the University of Essex, with a particular interest in the history of identification in Britain over the last 500 years.

Professor Higgs notes that the census has a long history and that it has often been considered by some to be intrusive. Moving to less intrusive means – such as processing administrative data – might help relieve individual burden, but might come at a cost to rigour or comparability.

There was probably as much information collected on individuals by officials in Tudor England as in today's world, and it was often more intrusive. Local Poor Law officials invaded homes to ensure that people were not harbouring possible charges on the parish rates; unmarried mothers in labour were interrogated as to the father of their child; moral and religious lapses were reported by neighbours to local church courts for punishment; and so on. This mainly communal surveillance was increasingly standardised from the late 18th century onwards by Whitehall and Parliament, through undertakings such as the decennial censuses from 1801 onwards.

The early censuses until 1831 somewhat continued the status quo, involving local parish officers providing headcounts to Parliament. No personal information left the locality. However, in 1841 there was a radical departure when census forms were introduced for householders to fill out. Until 1911 the information in these forms was standardised when copied into special books by census enumerators. This information was analysed in the central Census Office. Since all tabulation in the 19th century had to be done by hand, there was little possibility of using the enumerators' books to extract information on individuals. The returns were indeed effectively 'lost', only turning up in the attics of the Houses of Parliament in the post-war period. The use of punch-card tabulators supplied by the precursor of IBM from 1911, and electronic computers from 1961, allowed much more granular analysis of small areas and even individuals. During the second world war this allowed the state to mobilise labour for the military and for war production through the creation of a National Register.

Although the National Register was abandoned in 1952, the increasing ability of computers to merge census and other data to create personal profiles led to concerns about, and even outright rejection of, census-taking in the UK and abroad. This was especially the case in Germany, where census-taking was associated with the Nazi identification of Jews during the Holocaust. Recent proposals to replace the UK census altogether with profiling based on 'administrative data' held by central government would take this process one step further. The British state, it should be noted, has never promised its citizens census anonymity, or 'privacy', only data confidentiality.

The use of administrative data also raises the question of the comparability of census results. The paper-based censuses have always asked carefully worded questions, which have been backed up with standardised instructions. Will data collected from diverse sources have variables defined in standardised ways? Will changes in such data over time compromise the ability to reveal long-term trends across enumerations?

Society is therefore faced with a data system where data is increasingly difficult to meaningfully and sustainably trace. Decisions about when, where and how governance systems should intervene are becoming more difficult. At the same time, the significance of the potential benefits of effective management and use of data, and the potential risks associated with some uses, are fuelling calls for its societal impact to be addressed through governance, or a meaningful steer from politicians,[25] civil society, science[26] and industry.[27]

1.3 Process and context for this report

The UK benefits from a wealth of expertise in creating governance structures, processes or frameworks that can successfully negotiate the risks and benefits of rapid technological development. However, much of this expertise is fragmented across different sectors and groups.

25 Science and Technology Committee (Commons). 2015 *The Big Data Dilemma*. London: UK Parliament; Science and Technology Committee (Commons). 2015 *Robotics and Artificial Intelligence*. London: UK Parliament.

26 Royal Statistical Society. 2015 *The opportunities and ethics of Big Data*. London: Royal Statistical Society.

27 See for example the Partnership on Artificial Intelligence. https://www.partnershiponai.org (accessed 10 June 2017).

Therefore, in July 2016, the British Academy and the Royal Society initiated this review, with the aim of connecting debates across communities with interests in data governance. By bringing together stakeholders from a wide range of communities, each of which may be considering these issues in different contexts and with varied aims or assumptions, the Academies sought to connect discussions and better understand the needs of a 21st century data governance system.[28]

Drawing from input from across academia, industry, public sector and civil society,[29] this report is complemented by the following evidence about the shape and nature of the current governance landscape:

- Data Governance: Landscape Review
- Data Governance: Case Studies
- Data Governance: Public Engagement Literature Review
- Connecting Debates on the Governance of Data and its Uses
- Data Governance: Call for Evidence

This process of evidence gathering has identified key areas for attention, which are examined in the following chapters:

Chapter 2. Data governance: Tensions and disconnects looks at the current data governance landscape and the case for change, asking: What are the overarching reasons for concern and what specific tensions arise in the current system?

Chapter 3. Principles for Data Governance and Chapter 4. Essential functions and stewardship consider the interconnected nature of data processes, and the social and ethical opportunities and challenges that arise. There is an urgent need to steward the evolution of the governance landscape and establish a governance framework that is fit for the 21st century. These chapters set out the actions needed to establish such a framework and the principles that can act as beacons to shape the data governance environment.

28 British Academy and the Royal Society. 2016 *Connecting debates on the governance of data and its uses.* London: The Royal Society.

29 See Annex D: Evidence and engagement.

2
Data governance: Tensions and disconnects

Governance challenges need to be addressed in a timely manner if the overall system of data governance is to maintain public trust. Concepts that are core to public confidence in data governance – consent, for example – are increasingly contested, and new approaches to data management and data use are giving rise to pronounced and difficult-to-resolve tensions. The shifting ground around these concepts and tensions makes it difficult for society to frame meaningful questions about how to address or accommodate them. Meanwhile today's activities and decisions have potential long-term and cumulative effects.

Data-enabled technologies offer potentially massive benefits to society and individuals – from improving healthcare and treatment discovery, to better managing critical infrastructure such as transport and energy.

In the past, disruptive technologies such as the printing press or the introduction of weaving machines during the first industrial revolution, sparked major public controversy. While history does not enable us to predict the future, it suggests that the potential for controversies around data is very high. It also suggests that societies can act in advance to create well-founded responses that contribute to bringing the benefits of disruptive technologies into being.

Current experience suggests that, without a framework giving entrepreneurs and decision-makers sufficient confidence about acceptable uses of data, applications that would have been widely welcomed may be missed. Therefore, creating a framework suitable for the challenges of the 21st century will be central to securing the benefits of data.

Such a framework must enable society to navigate significant choices and dilemmas: it must consider who reaps the most benefit from capturing, analysing and acting on different types of data, and who bears the most risk. The framework must consider, as best as possible, the implications of the future nature and distribution of work, wealth and skills. It must ensure that the personalisation of news and views does not limit the diversity and richness of public debate or undermine those practices of checking and challenging claims that underpin democracy.

2.1 The case for change

Risk of public, data-related controversy

History has provided rich illustrations of how the widespread adoption of new technologies can increase public anxiety, or result in major public controversy, both of which risk hampering potential benefits. Examples of technologies that have attracted such controversy come from across scientific or technical domains, and include:

- **Nuclear power:** The world's first full-scale nuclear power station was opened at Calder Hall in Cumberland in 1956. The initial optimism over nuclear power began to falter a year after Calder Hall was opened, when a fire broke out in the nearby nuclear complex in Sellafield. Environmental campaigners also began to highlight the problems of disposing of nuclear waste. There was a fire in 1979

at Three Mile Island in the USA, followed by the Chernobyl nuclear disaster in the Ukraine in 1986, and public confidence in nuclear power was badly shaken.

- **Identity cards:** Identity card schemes were introduced in the UK for the first time in 1916. However, it was after their use in World War 1 that they became particularly controversial, and reached peak controversy in the 1950s. Identity cards were introduced during World War 1 as a way of increasing domestic security, but were generally regarded as a threat to civil liberties, and were discontinued at the end of the war. For similar reasons, they were re-introduced in 1939 and met with an equally unenthusiastic public response. Despite the objections, the government decided to continue the scheme in the face of the cold war and it was not until 1952 and that identity cards were abolished a second time.[30,31]

- **Railways:** The railway network became more controversial in the 19th century as development, investment and expansion occurred, and many people viewed them with a great deal of suspicion. People in rural communities feared the social changes that would emerge from the introduction of railways; operators of stage coaches and owners of canals feared it would destroy their livelihoods; and landowners who occupied estates in the path of the proposed lines believed trains would frighten the cattle, stop their hens laying eggs and spoil their view.[32]

Data infrastructures are not new (see Perspective 2: Historical context of data use), but that fact does not insulate them from controversy or provide immunity from the risk of a slow erosion of trust. These infrastructures house new technologies or changing practices, such as advanced machine learning or sophisticated algorithms, which may become controversial in some applications some time after their introduction. It is essential to address these new challenges and opportunities in a timely fashion.

30 Cannadine D. 2010 The nine lives of ID cards. *BBC News*. 18 June 2010. See http://news.bbc.co.uk/1/hi/magazine/8748441.stm (accessed 10 June 2017).

31 In 2002 the UK Government launched a six-month consultation on the re-introduction of identity cards. A wide range of arguments in favour of identity cards was put forward, but concerns about civil liberties and surveillance meant that most of the 7,000 responses were against the scheme. In May 2010, a total of 15,000 cards were in circulation but they were again abolished in 2010. See for example, HM Government. 2003 *Identity Cards: A summary of findings from the consultation exercise on entitlement cards and identity fraud.* London: The Stationery Office Limited. See http://webarchive.nationalarchives.gov.uk/20131205100653/http://www.archive2.official-documents.co.uk/document/cm60/6019/6019.pdf (accessed 10 June 2017).

32 Serpell N. 2010 Riches, rail and revolt. *BBC News*. 20 April 2010. See http://news.bbc.co.uk/1/hi/magazine/8631675.stm (accessed 10 June 2017).

If poorly handled, new ways to manage and use data can provoke a highly negative response, leading to missed opportunities in the intended and related application domains.[33] For example, the care.data centralised records system, which would have seen GP patient records opened to analysis by the National Health Service (NHS) and some third parties, could have provided an invaluable research resource and an important nationally strategic data set.[34] However, issues with management and communication, unrealistic expectations around the feasibility of rigorous anonymisation, and legal tensions and complications[35] all contributed to difficulties in the roll-out of this programme, which is now generally regarded as having failed (for further detail, see Perspective 3: The importance of public dialogue in Chapter 4).

Existing data governance concepts are under unprecedented strain

Notions such as accountability, agency, consent, privacy and ownership have a long history in governance practices across a diverse range of fields, including census collection, industrial research, customer loyalty card swipes, news articles, research data, web cookies and medical records (see Perspective: A short history of the census). However, these notions are becoming more difficult to maintain, due to the technical and social characteristics of today's approaches to data collection and use. Their meanings in policy, law and public discourse[36] have shifted, and will continue to do so in new and unpredictable ways. As a result, many of the concepts that sit at the core of public confidence in governance are no longer fit for purpose.

Some of the issues faced by notions of privacy, ownership and consent are set out below.

33 British Academy and the Royal Society. 2016 *Data Governance: Call for Evidence*. This report highlighted that missed opportunities for valuable and life-saving research are fuelled by lack of public trust (for example the Association of Medical Research Charities, Academy of Medical Sciences, National Data Guardian, the Wellcome Trust).

34 The potential importance of nationally strategic data sets such as these was identified at an important opportunity for the UK as part of this review's engagement with digital industries. See Annex D: Evidence and engagement.

35 Presser L, Hruskova M, Rowbottom H, Kancir J. 2015 Care.data and access to UK health records: patient privacy and public trust. *Technology Science*. 2015081103. See http://techscience.org/a/2015081103 (accessed 10 June 2017).

36 British Academy and the Royal Society. 2016 *Data Governance: Call for Evidence*. This report highlighted the lack of clear terminology as a major challenge for public debates. (See for example AMS, AMRC and ICO). Understanding Patient Data, set up in response to the Caldicott recommendations, attempts to address this by developing a new vocabulary and supporting conversations with the public, patients and healthcare professionals. See https://understandingpatientdata.org.uk/ (accessed 10 June 2017).

Privacy

The notion of privacy

Privacy is a deeply complicated, context-specific and multi-layered notion and its different aspects are often conflated.[37]

At a foundational level, different cultures and groups share different notions of privacy, setting boundaries about what is considered private or not. These boundaries also change depending on where an individual is – for example, at home or at work – and who is able to access the information. An individual's deliberate disclosure of personal information is an essential part of managing their identity[38] and how individuals perceive the privacy status of personal information is likely to differ depending on who it is shared with: friends, an insurer, a medical research facility, or a foreign government.

Privacy is not only about access of information, but can also include rights related to protection of one's identity or personal autonomy, as well as rights related to bodily integrity.[39] Additionally, the fact that something takes place in public, does not necessarily disqualify it from being private.[40] It is also worth noting that, although closely related to privacy, confidentiality is not the same thing: it is not dependent on the nature of the information and with whom it is shared, but upon the presence of a confidential relationship between the person who imparts information and the person who receives it.[41]

Compounding the differences between groups, attitudes to privacy are highly context specific and tied closely to the purpose for which data is used. For example, individuals may be more supportive of data use for public services than commercial application, or when there is less data sharing involved.[42] Or they may consider it acceptable to use individual data for one purpose, such as personalised career service, but not for improving transport services.[43]

37 O'Hara K. 2016 The Seven Veils of Privacy. *IEEE Internet Computing,* **20**, 2. See https://www.computer.org/cms/Computer.org/ComputingNow/issues/2016/05/mic2016020086.pdf (accessed 10 June 2017).

38 Foresight Future Identities. 2013 *Final Project Report.* London: The Government Office for Science.

39 Lipton J. 2015 Rethinking Cyberlaw (Edward Elgar, 2015) 141.

40 In the UK Supreme Court judgment in Catt, Lord Sumption referred to 'the recognition that there may be some matters about which there is a reasonable expectation of privacy, notwithstanding that they occur in public and are patent to all the world.' (R (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland [2015] UKSC 9 [10]).

41 Campbell v Mirror Group Newspapers Ltd [2004] 2 SC 457 (HL) [44].

42 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", (2014) 11:3 SCRIPTed 245 http://script-ed.org/?p=1667.

43 Ipsos MORI. 2014 *Public Attitudes to Science*; Ipsos MORI (research sponsored by Government Data Science Partnership, and Sciencewise). 2016 Public dialogue on the ethics of data science in government.

New challenges

As data and infrastructures become increasingly complex and interlinked, traditional thinking around privacy begins to falter. The ability to protect personally identifiable information is an essential component of trustworthy organisations. However, this can be difficult, if not impossible to achieve, even with the help of advanced privacy preservation techniques.[44]

Data is also now often collected without explicit knowledge.[45] It may be gathered from spheres previously thought of as private and combined with other datasets to reveal information which, in another context, is willingly shared through social media. The notion of privacy is also being stress-tested through the increased power of algorithms and their ability to infer and predict behaviour, something which is addressed in the Royal Society's report, *Machine Learning: the Power and Promise of Computers that Learn by Example*.

The need to protect personally identifiable data also needs to be balanced against the possibility that such data could be used to create public benefit (see section 2.2 for further discussion). The availability of data-enabled technologies might also intensify debates about acceptable level of risk to privacy in times of extraordinary circumstances. For example, humanitarian response organisations are increasingly turning to data to better respond to crises. Logistical information from companies operating in the region can supplement mapping and access data. The World Food Programme working with UN Global Pulse has demonstrated that data from mobile phone signals can be used to estimate poverty indices and food demand.[46] Proportionality tests may need to change when unexpected crises emerge or to prevent terrorism and illegal activity; however, such changes may also need to consider the future consequences of exceptional data sharing.

44 The Royal Society. 2016 *Progress and research in cybersecurity.* See https://royalsociety.org/topics-policy/%20projects/%20cybersecurity-research/ (accessed 10 June 2017).

45 British Academy and the Royal Society. 2017 *Public Engagement Literature Review*, 'Awareness' section.

46 Decuyper A *et al.* 2014 Estimating Food Consumption and Poverty Indices with Mobile Phone Data. *arXiv [cs. CY]*. See http://arxiv.org/abs/1412.2595 (accessed 10 June 2017).

Ownership

Uncertainties around the concept of ownership can be a barrier to effective trade and transfer of data, and leave individuals and organisations uncertain about their rights.[47]

Simplified versions of ownership, such as claiming that an individual should own all data concerning that individual, may create compelling soundbites but provide little direction in practice. Discussions of ownership sometimes confuse notions of 'intellectual property' with those of 'identity'. Data is often co-created and is capable of being silently captured, easily replicated, radically transformed, and cheaply transferred. This bears little resemblance to ownership in the way that one might own a house or a car.[48]

Such simplified notions can also create an expectation of compensation for use of data. Traditional models of ownership often do not recognise that value is typically derived from the combination and use of data rather than from individual data points. Creating appropriate mechanisms to apportion value will be a social and technical challenge and one that needs to consider how to balance asymmetries of power between different actors.[49]

Governance underpinned by a sophisticated understanding of ownership is also essential to extracting the commercial value of data. Recent work by the Royal Academy of Engineering highlighted the importance of data ownership across sectors and the ability to use data as a critical component in protecting it as an asset and realising its value[50] (See Perspective 4: Traded data as vital 21st century economic lubricant). In a post-Brexit world, with cross-border data flows underpinning over half of all global trade in services,[51] the importance of this is likely to increase.

47 The need for a greater articulation of 'the deal' between individuals and the organisations that hold data about them was highlighted by the ICO in its submission to the British Academy and the Royal Society. 2016 *Data Governance: Call for Evidence*.

48 English law courts have repeatedly held that data is not property, that conventional ownership rights therefore do not exist, and that there is no automatic right of access to the media or location where relevant data are stored. See for example: Osborne Clarke LLP. 2016 *Legal study on ownership and access to data*. Brussels: DG CONNECT, European Commission.

49 This was raised as a key challenges in the Review's engagement with the Civil Society. See Annex D: Evidence and engagement.

50 Royal Academy of Engineering and the Institution of Engineering and Technology. 2015 *Connecting data: driving productivity and innovation.* London: Royal Academy of Engineering.

51 See techUK submission to British Academy and the Royal Society. 2016 Data Governance: *Call for Evidence*. See https://royalsociety.org/~/media/policy/projects/data-governance/data-governance-call-collated-evidence.pdf (accessed 10 June 2017).

Perspective 4
Traded data as vital 21st century economic lubricant

Jim Norton is an independent director, policy adviser and public speaker. He is a Fellow of the UK Royal Academy of Engineering and has previously held senior roles in the private and public sectors.

Professor Norton argues that data must be mobile to realise relevant economic and social benefits, and that digital watermarking and new means of valuation might help us achieve this.

Appropriate access to data sets of the requisite quality is as essential to the development of the 21st century economy as coal and iron were to the industrial revolution. A welcome surge in the development of a broad swathe of applications of real economic and social value is being driven by the Open Data movement. The Open Data Institute and Alan Turing Institute are in the vanguard. Much useful data, however, remains locked away in proprietary corporate silos. Substantial barriers – technical, legal, structural and perceptual – contribute to this stasis, yet the value to all parties that could be liberated through sharing and trading is clear.

Shared data does not necessarily have to be 'free' data, but a legal framework for the secure trading of data sets is a prerequisite. Proprietary data 'owners' must be confident that they can retain control of their data and that valuable copies will not proliferate. Their rights must be enforceable. Techniques such as digital watermarking to uniquely identify data sets without damaging their utility and accuracy need further research. An analogy with the long use of unique, tiny, kinks in minor roads and paths in conventional geographic mapping data springs to mind.

New approaches are also required for assessing the financial value of data sets. This is a major challenge, since the intrinsic value increases dramatically if diverse sets can be effectively linked. Professor Sir Charles Bean's work on the Independent Review of UK Economic Statistics points to several potential approaches, but further targeted work is still required. As 21st century quoted companies increasingly depend on assets regarded as 'intangible', (including key data sets that are challenging to value using historic accounting techniques), new approaches are needed. This cannot be left simply to imputed valuation – lumped as part of 'goodwill' only at the point of corporate acquisition or disposal. Investors must demand better tools to assess the value of next-generation organisations that have few physical assets. A genuine 'balanced scorecard' of corporate value is increasingly essential.

Consent

Consent is one of the legal grounds for processing personally identifiable data in the current data protection regime.[52] However, genuine consent is difficult to achieve, and is often not sufficient to ensure adequate protection of individuals' interests. (See Perspective 5: Consent in a digital age). The application of consent suffers from what is often referred to as the 'transparency paradox'.[53] Consent requires transparency of what is being consented to. Such transparency has to be meaningful, and the mere disclosure of information is not enough.[54] Anything too long or complex is unlikely to be broadly understood or read yet making a summary widely comprehensible often discards the details that people care about.

As data collection become less about the active 'giving' of information and more about information captured as a by-product of interactions with products, services, the physical environment and each other, it is increasingly difficult for individuals to provide meaningful consent to share data.[55] It is almost impossible for any one person to keep track of what data is collected about them and how it will be used.

52 For more detail on the role of consent in the data protection regime, see British Academy and the Royal Society. 2017 *Data Governance: Landscape Review.* London: The Royal Society.

53 Nissenbaum H. 2011 A contextual approach to privacy online. *Daedalus* 140, 4. See http://www.mitpressjournals.org/doi/10.1162/DAED_a_00113 (accessed 10 June 2017).

54 See for example the notion of 'intelligent openness' which requires data to be accessible, intelligible, assessable and usable. The Royal Society 2012. *Science as an Open Enterprise.* London: The Royal Society. See https://royalsociety.org/~/media/policy/projects/sape/2012-06-20-saoe.pdf (accessed 10 June 2017).

55 This is a particular issue in commercial settings where the standard of informed consent is through 'ticking and clicking' terms and conditions, but which often happens without them being read or understood.

The rare settings where the notice-and-consent paradigm functions well – for example, aspects of healthcare[56] – work because there is greater trust in the system as a whole.[57] This highlights the importance of ensuring that the institutions and processes to engender trust are in place. There are various examples of data governance structures which recognise that genuine consent is sometimes unworkable, and where additional safeguards need to be put in place. For example, the Administrative Data Research Network (ADRN) allows accredited researchers to access de-personalised administrative data for social and economic research.[58,59]

It is also important to note that consent is not always sufficient. Current notions are of consent on an individual basis. However, some forms of information, such as the human genome, may contain potential future insights about issues such as health and wellbeing not just about one individual but also about their family.

Also, as it is possible to infer sensitive characteristics, such as depression, from wearable devices[60] one may imagine a group of users who share potentially sensitive health or lifestyle attributes. If only some users consent to data processing, it might still be possible to predict that characteristic for all similar users. As it stands, data protection law alone insufficiently protects individuals in these cases from evolving insights that may affect their lives.[61]

56 In submissions to the British Academy and the Royal Society. 2016 *Data Governance: Call for Evidence*, the National Data Guardian is highlighted as an important part to establish trust within healthcare, while there are calls for more coordination of health data with other sectors. See for example responses from the Association of Medical Research Charities and the Wellcome Trust, https://royalsociety.org/~/media/policy/projects/data-governance/data-governance-call-collated-evidence.pdf (accessed 10 June 2017).

57 Research commissioned by the Royal Statistical Society suggests that there is a general 'data trust deficit', and that public support for sharing personally identifiable data depends very much on who it is being shared with, and for what reason. *Royal Statistical Society. 2014 Royal Statistical Society research on trust in data and attitudes toward data use/data sharing* See http://www.statslife.org.uk/images/pdf/rss-data-trust-data-sharing-attitudes-research-note.pdf (accessed 10 June 2017).

58 For example, data held by the ADRN can only be accessed by accredited researchers with specialised training and can only be accessed in secure environments. For further information, see ADRN. n.d. Ethics and administrative data. See https://adrn.ac.uk/media/174021/ethics-and-administrative-data-guidance_00_09_pub.pdf (accessed 10 June 2017).

59 Work by the Medical Research Council and the Wellcome Trust on data safe havens also considered different models of secure environments for handling data and sets out the challenges that need to be addresses. See The Academy of Medical Sciences. 2014 *Data in safe havens.* See http://www.acmedsci.ac.uk/viewFile/53eb4d247ef80.pdf (accessed 10 June 2017).

60 For example, see Fedor S, Chau P, Bruno N, Picard RW, Camprodon J, Hale T. 2016 Can we predict depression from the asymmetry of electrodermal activity? *Journal of Medical Internet Research*. **18**, 12. See http://dx.doi.org/doi:10.2196/iproc.6117 (accessed 10 June 2017); Sano A et al. 2015 Recognizing academic performance, sleep quality, stress level, and mental health using personality traits, wearable sensors and mobile phones. In: *IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks*. See http://dx.doi.org/doi:10.1109/BSN.2015.7299420 (accessed 10 June 2017).

61 See for example: Kosinski M, Stillwell D and Graepel T. 2013 Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences* **110**, 15: 5802-5805; or Hildebrandt M. 2008 Profiling and the identity of the European citizen. In: Hildebrandt M, Gutwirth S (eds) *Profiling the European Citizen*. Heidelberg: Springer.

Perspective 5
Consent in a digital age

Hannah Knox is Lecturer in Digital Anthropology and Material Culture at University College London.

Dr Knox sets out the approach to consent used in anthropological research, which highlights the importance of clear responsibility and securing future access to research. It also acknowledges the social aspect of consent, which needs to be an ongoing process that cannot be justifiably overridden by the pursuit of knowledge alone.

One of the key challenges of new forms of data revolves around the twin issues of consent and anonymity. Data is now produced, circulated and used in a variety of ways by different institutions and individuals. Currently individuals are asked to sign complex terms and conditions when signing up to a service. However, their use of that service may change significantly over time, the uses of the data produced by their interaction with that service are often not transparent, and the linking of data has been shown to potentially compromise anonymity. Together these issues imply that a better way of approaching ethical questions of consent and anonymity must be found. Rather than approaching consent from just a legal or technical perspective, it may be that we need a more human-centred understanding of what consent is and how it can be established.

Anthropologists have long had to concern themselves with the complex social and cultural implications of seeking consent and ensuring anonymity. As with users of digital services, anthropological research subjects often engage with researchers, and thus produce data over long periods of time. Anthropological research data is frequently used many years into the future and its uses may be unanticipated at the time of its collection. In addition, information from a wide range of individuals and spheres of social interaction are frequently brought together in a single research study, which potentially compromises individual anonymity. Anthropologists also recognise that consent is not a universal principle and that different cultural and legal systems have different ideas about who or what can be a consenting subject.

Traditionally anthropologists have responded to these challenges by aiming to work within a clear set of ethical guidelines that acknowledge the complexity of consent. For example, the Ethical Guidelines of the Association of Social Anthropologists of the UK and Commonwealth establishes the following principles for dealing with consent as a social contract:

a) Anthropologists as collectors of data are understood to have primary responsibility for protecting research participants, honouring trust and ensuring that, as far as possible, they guard against predictable harmful effects.

b) Consent is understood to be an ongoing and socially contingent process that necessarily has to be revisited at different moments in the research process.

c) Research sites must be left in a state that means they can be accessed by other researchers in the future.

d) Anthropologists are understood to have no special entitlement to study all phenomena. The advancement of knowledge and the pursuit of information are not in themselves sufficient justifications for overriding the values and ignoring the interests of people studied.

e) Extended embargo of research materials may enable the use of research data for future researchers, while honouring present commitments.

While new forms of research with digital data, such as social media feeds, and self-quantification data open up new ethical questions, basic foundational ethical principles remain relevant as we are still working with relationships between human subjects. These ethical guidelines highlight the importance of assessing who should take responsibility for ethical implications of data use: individuals, governments or corporations? They also open up the question of how to assess whether consent to different kinds of data use has truly been achieved under a variety of different conditions.

Uncertainties are accumulating and compounding

Through engagement with industry, academia, the third sector and policymakers, we have identified a range of uncertainties and tensions emerging from the ways data is managed and used. At present, the UK and other societies do not stand fully prepared to respond as effectively as they could. As these uncertainties evolve and accumulate, accommodating them becomes increasingly daunting. Acting on them is necessary, but doing so in an unconsidered way may bring long-term, cumulative and difficult-to-foresee effects.

Some of the current uncertainty stems from the challenge to concepts, such as accountability, agency, consent, privacy and ownership, which underpin systems of governance. Further uncertainty is caused by regulatory regimes lacking the agility required in a rapidly changing world. Current systems appear to require individual grievances about new technologies to reach a critical point before uncertainty can be addressed and clarification sought. (See Box 3: Keeping pace with technology).

Box 3: Keeping pace with technology

Social and technological developments, as well as unusual or unexpected examples, are likely to stress the principles and the governance systems derived from them.

For legislative concerns, the judiciary provides important means of clarification, but this is not always sufficient, for several reasons. First, it often requires a grievance to be so strong that it is taken to court, but is not settled along the way. Many aspects of data protection law are unclear precisely because so few cases get clarified in this way. For example, one of the most notable instances was 'the right to be forgotten' which saw a Spanish citizen arguing that the availability of an auction notice of his repossessed home on Google search was a breach of privacy. The citizen took the case to the European Court of Justice which ruled that, based on requests from individuals, certain results should be removed from search engines. There are consistent calls for laws to be 'technology-neutral', yet technology-neutral statutes require judicial interpretation to clear up the uncertainties of how they might be applied.

Second, the period of time before judicial clarification is reached can be a difficult period of uncertainty. Amid this uncertainty, organisations investing in infrastructure and training to meet regulations can do so sub-optimally. For example, the 'right

to explanation'[62] of any decision affecting individuals which has been reached algorithmically in the General Data Protection Regulation (GDPR)[63] is limited in practical settings without judicial clarification.[64] It all depends on how it is interpreted in the future by national and European courts.

At the time of such clarification, in the context of machine-learning technology, data controllers and processors may require considerable time and investment to alter their systems. In some cases, this might not be possible at all.

Some sub-judicial clarification functions are already partially built into data-relevant legislation. The clarification of data protection legislation in the context of new technologies is currently undertaken by a combination of individual data protection supervisory authorities, such as the UK's Information Commissioner's Office (ICO), in addition to the collaborative Article 29 Working Party (A29WP),[65] which consists of representatives from supervisory authorities in the Member State and provides the European Commission with independent advice on data protection.[66] The future of the UK's role in these arrangements is unclear in the context of the vote to exit the European Union.

Yet, since the A29WP is only responsible for data protection law, its advisory opinions clarifying the use of new technology within a regulatory context is inherently limited. Data protection law is only a small portion of the relevant legal landscape, let alone the broader relevant governance landscape including regulators with mandates touching on aspects of data governance, such as the Competition and Markets Authority,[67] Ofgem, Ofcom and the Financial Conduct Authority (FCA).

---

62 Kobsa A. 2001 Tailoring Privacy to Users' Needs. In: M Bauer et al. (eds) *User Modeling*, Lecture Notes in Computer Science, Springer; Goodman B, Flaxman S. 2016 European Union regulations on algorithmic decision-making and a 'right to explanation'. See https://arxiv.org/abs/1606.08813 (accessed 10 June 2017); The Guardian view on computers and language: reproducing bias. *The Guardian*. 14 April 2017. See https://www.theguardian.com/commentisfree/2017/apr/14/the-guardian-view-on-computers-and-language-reproducing-bias (accessed 10 June 2017).

63 The GDPR will come into force from 25 May 2018 and the ICO has confirmed that it will replace the current legislation, regardless of UK's exit from the European Union.

64 Bygrave LA. 2000 Minding the machine: Article 15 of the EC Data Protection Directive and automated profiling. *Privacy Law & Policy Reporter,* **7**, 67–76; Hildebrandt M. 2012 *The dawn of a critical transparency right for the profiling era* in Bus J *et al.* (eds) *Digital Enlightenment Yearbook* 2012, IOS Press; Wachter S *et al.* (forthcoming) *Why a right to explanation does not exist in the General Data Protection Regulation*. Oxford: International Data Privacy Law.

65 The Article 29 Working Party coordinates the data protection supervisory authorities in each state. Under the GDPR, this body will become the European Data Protection Board (EDPB).

66 Norway, Iceland and Liechtenstein, as well as the European Data Protection Supervisor, also sit in this group.

67 For more information, see Competition & Markets Authority. 2015 *Commercial use of consumer data.* HM Government. See https://www.gov.uk/government/consultations/commercial-use-of-consumer-data (accessed 10 June 2017); also see Authorité de la concurrence; Bundeskartellamt. 2016 Competition law and data. http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf (accessed 10 June 2017).

Without the frameworks to give researchers, entrepreneurs and decision-makers sufficient confidence about acceptable uses of data (in the eyes of the law and the public) applications that would have been widely welcomed may be missed.[68]

There are also major potential social and economic transformations fuelled by data-enabled technologies that society does not yet know how to best navigate. One illustration of this is in the current debates about the power of automation to transform the world of work, which pose questions about which parts of society will, and should, benefit.[69] The next section of the report illustrates the mounting uncertainty, through a framework of tensions.

2.3 Tensions in data management and data use

Many of the choices that society will need to make as data-enabled technologies become more widely adopted can be thought of as a series of pervasive tensions, which illustrate the kinds of dilemmas that society will need to navigate.

Box 4 gives a non-exhaustive list of these tensions. This list will undoubtedly evolve in unpredictable and unanticipated ways. What can be stated with certainty is that the use of data-enabled technologies will continue to give rise to situations where important choices will need to be made. These choices will usually resist simple maximisation or optimisation, though technological developments may change the nature of these tensions in future.

68 This was identified as a key challenge as part of evidence gathering for this review, for example, as a barrier for ensuring innovation, data sharing and valuable research.

69 See work by the Royal Society on Machine Learning and further work planned. See https://royalsociety.org/topics-policy/projects/machine-learning/ (accessed 10 June 2017).

Box 4: Framework for social and ethical tensions[70]

- Using data relating to individuals and communities to provide more effective public and commercial services, while not limiting the information and choices available.
- Promoting and distributing the benefits of data use fairly across society while ensuring acceptable levels of risk for individuals and communities.
- Promoting and encouraging innovation, while ensuring that it addresses societal needs and reflects public interest.
- Making use of the data gathered through daily interaction to provide more efficient services and security, while respecting the presence of spheres of privacy.
- Providing ways to exercise reasonable control over data relating to individuals while encouraging data sharing for private and public benefit.
- Incentivising innovative uses of data while ensuring that such data can be traded and transferred in mutually beneficial ways.
- Making the most of the ability of algorithms to provide accurate outcomes beyond the human ability while ensuring appropriate levels of interpretability and transparency, and allowing for systems of accountability to be put in place.
- Facilitating debate and engagement while ensuring that such debate is meaningful (reciprocal, has the capacity to shape policy and includes an open and accessible articulation of competing values at stake).

Where questions are tricky and where diverse individuals and communities do not agree on the societal ends or how best to achieve them, democratic mechanisms to resolve them are needed. This requires value judgments to be made continuously, inclusively, collectively and with careful regard for context.

Because the challenges brought on by the tensions are pervasive, interconnected, collective, value-laden and technically daunting, they stubbornly resist linear, ad-hoc policy solutions. These tensions are rarely addressed directly when developing data governance strategies. This may be an appropriate response in some contexts,

70 Throughout the engagement and evidence-gathering phase of the review, these have been discussed and refined by a range of different communities. See Annex D: Evidence and engagement.

and may work well when the stakes are low, but it is likely to become increasingly problematic as issues around data appear in more locations and more sectors with unprecedented speed.

This, in turn, can increase the risk of potentially undesirable ways to manage and use data, as well as the risk of forgoing important potential benefits. Societies must identify important tensions, balances and dilemmas where they exist, and navigate them in the best way possible, alongside further research in the theory of balancing constraints.[71]

In this section, we examine selected tensions and illustrate them with examples of the challenges they present.

Tension: Using data relating to individuals and communities to provide more effective public and commercial services, while not limiting the information and choices available.

The greater the 'data exhaust'[72] that individuals and communities leave behind, the greater the opportunities for tailoring public and commercial services and making them more efficient to suit particular needs and preferences. Yet, this same tailoring could be restrictive to the way individuals engage in the world around them.

For example, the UK Government handles 1.5 billion transactions with business and citizens annually[73] and analysis of this administrative data can help reduce the cost of public services, increase understanding of socio-economic issues and help make better policy.[74] However, much of this data contains information related to individuals. It will often be of a sensitive nature and its management and use may cause public concern.[75] The data is generated for a specific administrative purpose, and citizens might not be aware of, or agree to it being used for research purposes or as part of a public resource. This may be particularly true if there is a risk of

71 See for example: recent additions by Kleinberg J, Mullainathan S and Raghavan M. 2016 Inherent trade-offs in the fair determination of risk scores. *arXiv*:1609.05807 as well as Chouldechova A. 2016 Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. arXiv preprint arXiv:1610.07524.

72 The data generated by an individual through daily activities.

73 Laurie G and Stevens LA. 2016 Developing a public interest mandate for the governance and use of administrative data in the United Kingdom, *Journal of Law and Society*, **43**, 360–392. See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2822556 (accessed 10 June 2017).

74 Administrative Data Research Network. See https://adrn.ac.uk/research-impact/research/ (accessed 10 June 2017).

75 The *Data Governance Public Engagement Review* (2017) found that data science to profile and target certain sectors of society raised concerns, particularly in cases using administrative data, and the use of data to segment groups.

individuals being exposed to potential harm or the possibility that inequalities built into the system are perpetuated.

In commercial settings, the potential for personalisation comes with benefits as well as risks to autonomy.[76] It is possible to narrowly target products and services, making it easier for an individual to seek out more suitable services and products and navigate an environment of information overload. However, in some cases these benefits come with the risks of undesirable statistical stereotyping and profiling.[77]

A dialogue exercise undertaken as part of the Royal Society's work on machine learning considered the ability for machine learning to personalise options. There was concern among participants that this personalisation might, in some cases, restrict their freedom of choice. Conversely, participants also considered that machine learning would help improve their experiences in some circumstances.[78]

This has an effect on an individual level, where using historical data to guide future decisions may reproduce problematic patterns – for example, being more or less likely to be shown advertisements for high-level jobs based on gender.[79] There is also a societal level effect, with some arguing that a thriving democracy relies on interacting with a diversity of political views or values.[80] An example of this is the current controversy surrounding the use of data analytics in political campaigning to target specific groups or areas to the exclusion of others.[81]

76 Yeung K. 2016 'Hypernudge': Big data as a mode of regulation by design. *Information, Communication & Society* 20: 1: 118–36.

77 The Royal Society 2017. *Machine learning: the power and promise of machines that learn by example.* London: The Royal Society. See https://royalsociety.org/topics-policy/projects/machine-learning/ (accessed 10 June 2017).

78 Ipsos MORI (research sponsored by the Royal Society). 2017 *Public Views of Machine Learning.* See https://royalsociety.org/~/media/policy/projects/machine-learning/publications/public-views-of-machine-learning-ipsos-mori.pdf (accessed 10 June 2017).

79 Gibbs S. 2015 Women less likely to be shown ads for high-paid jobs on Google, study shows. *The Guardian*. 8 July 2015. See https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study (accessed 10 June 2017).

80 See for example: Sunstein R. 2017 *#Republic: Divided Democracy in the Age of Social Media*. New Jersey: Princeton University Press.

81 The ICO launched an investigation into the use of data analytics for political purposes in May 2017. However, some argue that, as data protection is limited to the use of personally identifiable information, it will struggle to address questions involving the identification of larger groups, based on, for example, age or geography.

Tension: Promote and distribute the benefits of data management and data use fairly across society while ensuring acceptable level of risks for individuals and communities.

Data-enabled technologies offer the promise of benefits for individuals and society. They present choices about how to best distribute those benefits across society. For example, the greater automation of the workplace is likely to result in productivity gains, and the creation of new global data markets is going to produce new powerful economic actors. In both of these cases, how society chooses to act will help determine who stands to gain and lose from these changes. (See Perspective 6: Data use, equality and society).

Key questions that can arise in this context include when individual interests should be prioritised over public good, or when public good should take priority over commercial interest. An example of when interests may be in tension are when firms hold data that can provide public good, often when aggregated across organisations. This could include information on cybersecurity breaches, manufacturing performance or logistical information relevant to humanitarian response.[82]

One instance of this included a Japanese manufacturer of heavy machinery that had been remotely collecting global monitoring data from their equipment.[83] These data sets contained commercially sensitive information about individual firms, such as how hard their operators worked, but was also highly sought after for the fine-grained insights it offered into regional economic patterns. When it is the case that firms hold commercially sensitive data of potential social value, where is the incentive to trade such data? Apart from the contractual issues, it may not be sufficiently profitable for a firm to want to share their data. Even if a firm did see profitability in this, if societal pressure is applied without providing safeguards around legal liability for disclosing commercially sensitive information, would companies consider destroying this data rather than storing it?

These broad questions are not unique to use of data-enabled technologies. However, they are perhaps exacerbated by the fact that underlying concepts, such as privacy and ownership, which many relevant governance responses rest on and which inform public debate, are under unprecedented strain.

82 Please see Data Governance: Case studies section on Data in Humanitarian Crisis.

83 Lucas L, Lewis L. 2016 Wanted: Japan digger group's secret trove of global economic data. *Financial Times*. 28 November 2016.

Perspective 6
Data use, equality and society

Sabina Leonelli is Professor of Philosophy and History of Science at the University of Exeter and Co-Director of the Exeter Centre for the Study of the Life Sciences.

Professor Leonelli explains how data linkage and interpretation are not neutral activites but heavily shaped by human decisions and global inequalities. She warns that, since not everyone is equally involved in data collection, processing and use, there is a risk of exacerbating existing digital divides.

Data production and dissemination channels such as social media, governmental databases and research repositories operate in a globalised, interlinked and distributed network. The power of any one dataset to yield knowledge lies in the extent to which it can be linked with others: this is what lends high epistemic and commercial value to digital objects such as global positioning system (GPS) locations or sequencing data, and what makes extensive data aggregation from a variety of sources into a highly effective surveillance tool.

The interconnected and international nature of data dissemination makes it impossible for any one individual to retain oversight over the quality, import and potential social impact of the knowledge being produced. Many individuals, groups and institutions end up sharing responsibility for the social outcomes of specific data uses. A key challenge for data governance is to find mechanisms for allocating responsibilities across this complex network, so that any fraudulent, unethical, abusive or discriminatory actions can be singled out, corrected and appropriately sanctioned.

To this aim, it is crucial for policymakers to recognise that there is *no simple technological fix* for monitoring the social impact of data use. Computational tools for data tracking and monitoring continue to improve at breathtaking speed, and yet they unavoidably *rely on human decisions* about what counts as data in the first place and how data should be ordered, labelled and visualised. These decisions are particularly significant given that not all data are equally easy to digitally collect, disseminate and link through existing algorithms, resulting in a *highly biased data pool* that does not accurately reflect reality (and in some cases actively distorts it). Far from being purely technical, data management decisions therefore affect what kinds of uses data can be put towards, and its implications.

At the same time, the existing distribution of resources, infrastructure and skills determines *high levels of inequality* in public participation to the production, dissemination and use of data. In government, academic research and industry, big

players with large financial and technical resources are leading the development and uptake of data analytics tools, leaving the rest of society at the receiving end of innovation. Contrary to popular depictions of the data revolution as harbinger of transparency, democracy and social equality, the *digital divide* between those who can access and use data technologies and those who cannot continues to widen. The vast majority of the population is thus encouraged to provide more and more personally identifiable data for access to digital services, but does not have the means to consider the multiplicity of uses to which such data can be put and the potential for negative repercussions on themselves and their communities.

Given this fraught landscape, governing data use requires a participatory approach to the production and oversight of tools for data management and analysis. Technicians need to work alongside people who may not have technical skills in data science, but who do have the experience and expertise to make informed and considered decisions around data use and its social implications. Data processing strategies and tools should never be developed separately from the situations of data use where ethical and social concerns emerge.[84]

Tension: Promote and encourage innovation, while ensuring that it addresses societal needs and reflects public interest.

Innovative uses of data offer great potential for the UK economy. It is estimated that £66 billion of business and innovation opportunities could be generated through effective use of data.[85] To keep step with the pace of change and remain competitive, innovation should be encouraged. At the same time, direction is needed to help guide innovation in areas where there are urgent needs.[86]

In many instances these are not seen as conflicting objectives, but as data-enabled technologies have increasingly large and uncertain social, economic and ethical consequences, getting the balance right will be critical.

84 Relevant highlighted works from Dr Leonelli include Bezuidenhout L *et al.* 2017 Beyond the digital divide: Towards a situated approach to open data. *Science and Public Policy*, forthcoming; Leonelli S. 2016 Locating ethics in data science: responsibility and accountability in global and distributed knowledge production. *Philosophical Transactions of the Royal Society: Part A*. **374**: 20160122; Leonelli S. 2016 *Data-centric biology: A philosophical study.* Chicago, IL: Chicago University Press; Leonelli S. 2014 What difference does quantity make? On the epistemology of big data in biology. *Big Data and Society* **1**: 1–11.

85 Parris S *et al.* 2016 *Digital Catapult and productivity: A framework for productivity growth from sharing closed data.* Cambridge UK: Rand Corporation. See http://www.rand.org/pubs/research_reports/RR1284.html (accessed 10 June 2017).

86 For discussion on important research challenges, see the Royal Society *Machine Learning: the power and promise of computers that learn by example* (2017) and *Progress and research in cybersecurity* (2016).

Models of how to achieve this balance are emerging and gaining traction. For example, Responsible Research and Innovation (RRI) is a tool to steer responsible and successful innovation that has gained increasing attention in the last few years.[87] Its intention is to bring issues related to research and innovation into the open, to anticipate their consequences, and to involve society in discussing how science and technology can help create a desirable future.[88] In practice, RRI is implemented as a package that includes multi-actor and public engagement in research and innovation.

Industry is also playing an active role in this space. For example, the Partnership on Artificial Intelligence to Benefit People and Society[89] which was founded by some of the biggest global technology companies, has a stated goal to advance public understanding and awareness of AI and its potential benefits and costs. It also aims to support research and recommend best practices in a range of areas including ethics, fairness, and inclusivity, and promote the trustworthiness, reliability and robustness of the technology.

2.3 Strained systems of governance and the responses required

The evidence we have gathered for this project demonstrates clearly that today's systems for governing data are under stress; this is hardly surprising given the speed of changes underway. We are not arguing that there is an immediate failure in law.[90] Equally, we are strongly of the view that, while the current governance architecture provides a great deal of what is necessary for the here and now, there are very clear gaps between today's framework and what is needed to meet the future challenges of data governance in the 21st century.

87 In particular, within the European Commission's Science With And For Society programme, in the context of the Horizon 2020 strategy.

88 See for example Owen R, Macnaghten PM, Stilgoe J. 2012 Responsible research and innovation: from science in society to science for society, with society. *Science and Public Policy*. **39** (6): 751–760. See http://dx.doi.org/doi:10.1093/scipol/scs093 (accessed 10 June 2017); Stilgoe J, Owen R, Macnaghten P. 2013 Developing a framework for responsible innovation". *Research Policy*. **42**: 1568–1580. See http://dx.doi.org/doi:10.1016/j.respol.2013.05.008 (accessed 10 June 2017).

89 Partnership on AI. 2016 *Industry leaders establish partnership on AI best practices* [press release] 28 September 2016. See https://www.partnershiponai.org/2016/09/industry-leaders-establish-partnership-on-ai-best-practices/ (accessed 10 June 2017).

90 British Academy and the Royal Society. 2017 *Data Governance: Landscape Review*. London: The Royal Society.

However, emerging anxieties about the opportunities and risks of this rapidly changing landscape have led some to desire specific governance responses.[91]

The Royal Society's report *Machine Learning: The Power and Promise of Computers that Learn by Example* sets out why it is not appropriate to set up governance structures for machine learning per se. While there may be specific questions about the use of machine learning in specific circumstances, these should be handled in a sector-specific way, rather than via an overarching framework for all uses of machine learning. Some sectors may have existing regulatory mechanisms that can manage, while others may not have these systems.[92]

The range and variety of tensions set out above demonstrate once again the importance of context. While there will be challenges for the governance of data use that are general in nature, many of them (and their implications) are likely to be highly specific. For example, the use of data to create personal recommendations for online shopping creates different forms of benefit and risk, and involves different forms of agency from the use of data to inform healthcare decisions. It would be wrong to attempt to govern them in the same way. The primacy of purpose means that most forms of governance are, and should be, specific to context.

At the same time, new ways of using data means that a framework designed for one sector may have implications for data use in another; transport data may inform health choices, or commercial data help target public services. There is great scope for benefit here, but also great challenges relating to common underlying themes such as privacy, consent, bias and quality. As different sectors grapple with these challenges, there is much to be learned from each other.

This situation requires two types of response:

First, a renewed governance framework needs to ensure trustworthiness and trust in the management and use of data as a whole. This holistic need can be met through a set of high-level principles that would cut across any data governance attempt, helping to ensure confidence in the system as a whole. These are not

91 See for example, Garside J. 2016 Labour calls for closer scrutiny of tech firms and their algorithms. *The Guardian* 19 December 2016. See https://www.theguardian.com/business/2016/dec/18/labour-calls-for-regulation-of-algorithms-used-by-tech-firms (accessed 10 June 2017); UK Parliament. 2017 Debates on the Digital Economy Act 2017 http://services.parliament.uk/bills/2016-17/digitaleconomy.html (accessed 10 June 2017); Mulgan G. 2016 A machine intelligence commission for the UK. *Nesta blogs*. 22 February 2016. See http://www.nesta.org.uk/blog/machine-intelligence-commission-uk (accessed 10 June 2017).

92 The Royal Society. 2017 *Machine learning: the power and promise of computers that learn by example.* London: The Royal Society. See https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf (accessed 10 June 2017).

principles to fix definitively in law, but to visibly sit behind all attempts at data governance across sectors, from regulation to voluntary standards.

Second, it is necessary to create a body to steward the evolution of the governance landscape as a whole. Such a body would not seek to duplicate the efforts of any existing bodies, but would ensure that the complete suite of functions essential to governance and to the application of the Principles for Data Governance is being carried out across the diverse set of public and private actors involved in data governance. Because many types of data – or technologies making use of data – have significant or contested social values embedded within them, such a stewardship body would need strong capacities for public engagement, deliberation and debate. We see this body as an essential step in stewarding the landscape during the period of particularly disruptive transition which society faces for the coming years.

Calls to address the challenges of increasing use of data, emphasising the importance of open dialogue, trust and greater coordination were made in 2005 by the Council for Science and Technology.[93] Twelve years on, the issue is now even more urgent.

93 Council for Science and Technology. 2005 Better use of personal information: opportunities and risks. See http://webarchive.nationalarchives.gov.uk/20130705054945/http:/www.bis.gov.uk/assets/cst/docs/files/cst-reports/05-2177-better-use-personal-information.pdf (accessed 10 June 2017).

3
Principles for Data Governance

A set of high-level principles is needed to visibly shape all forms of data governance. We propose four action-orientated principles, with an overarching guiding principle, to provide a vision for a 21st century data-enabled society.

Drawing on insights from general principles in law and good governance practice across other areas of society, we propose the introduction of four high-level principles informed by one overarching guiding principle.[94]

These principles are not detailed prescriptions for action, but rather serve as guides, checks and prompts that may be formalised to greater or lesser degrees in different sectors and applications. They should underpin sector- and context-specific governance models and tools used in different areas of practice – whether in the form of codes of ethics, technical, operational or legislative standards, or technological solutions such as privacy by design.

These underpinning principles are intended to apply to the individual components of the disconnected governance landscape, yet provide the overarching vision that connects the various parts of data governance across different sectors together. They allow scope for diverse and bespoke governance solutions relevant to the sector and purpose, while providing a visible point of connection to build trust and confidence in the system as a whole.

They aim to orient and guide those evaluating existing governance mechanisms and those considering new forms of governance. In this context, principles should be simple and memorable, to ensure they are amenable to application, as – above all – their application is what matters. It is inevitable that argument and debate will be needed to determine their full meaning, as well as the actions surrounding them.

The overarching principle is that systems that govern data should **promote human flourishing**. Four additional principles reflect the need to enable well-founded debate on the tensions discussed in the report, and help visibly shape all forms of data governance. They are that the systems of data governance should:

- **protect individual and collective rights and interests**
- **ensure that trade-offs affected by data management and data use are made transparently, accountably and inclusively**
- **seek out good practices and learn from success and failure**
- **enhance existing democratic governance.**

We expand on each of these principles below.

94 These principles include a commitment to respect fundamental rights and freedoms such as those enshrined in the European Convention on Human Rights which include: the right to freedom of expression; the right to a fair trial; the right to peaceful enjoyment of property; and the right to respect for private and family life and which therefore underpin the way in which constitutional democracies seek to govern.

Promote human flourishing

The promotion of **human flourishing** is the overarching principle that should guide the development of systems of data governance. This principle is intended to provide an orientating mission that has 'the human' at its centre. At moments of contention, it should serve to reflect the fundamental tenet that society does not serve data, but that data should be used to serve human communities.

The concept of 'human flourishing' is deliberately broad: it emphasises the nature of human wellbeing, as well as recognising the importance of context and the role of competing interests and values. Its resistance to a simple, widely shared definition should serve to emphasis the centrality of continued democratic definition.

Flourishing therefore has several features which make it a useful concept to guide data governance:

- Flourishing can be applied as a test to the use and management of all data, whether personally identifiable or not. While the recital of the GDPR notes that the 'processing of personal data should be designed to serve mankind',[95] it is important to recognise that non-personally identifiable data can also be highly significant to human flourishing, supporting a growing economy and prompting public benefits in areas such as health, infrastructure and the environment.

- Flourishing is multidimensional, as is data governance. In policies drawing from concepts relating to wellbeing, flourishing creates requirements beyond 'life satisfaction' or 'happiness' to define some core human purposes or goals,[96] and to assess the extent to which the capabilities required to meet those goals are present.[97, 98]

- Flourishing is dynamic and context-specific. It is not possible to pre-define static human goals, but it is possible to get better at defining relevant measures for particular situations and contexts. The active and inclusive effort needed to define flourishing is its strength, and makes it more effective and robust than constant, single dimension views of human welfare. The act of arriving at a definition should be a familiar practice within businesses, civil society organisations, regulators or sectoral bodies.

95 GDPR, recital 4.

96 Multidimensional measures inspired by the concept of flourishing are already popular in development policy. See the three-dimensional Human Development Index (HDI), inspired by Amartya Sen's Capability Approach, as well as the Multidimensional Poverty Index (MPI) developed for the UN Development Programme, and the Oxford Poverty & Human Development Initiative. See http://www.ophi.org.uk (accessed 10 June 2017).

97 OECD. 2013 *Guidelines on Measuring Subjective Well-being*, OECD Publishing. See http://www.oecd-ilibrary.org/economics/oecd-guidelines-on-measuring-subjective-well-being_9789264191655-en (accessed 10 June 2017).

98 Allin P, Hand DJ. 2014 *The Wellbeing of Nations: Meaning, Motive, and Measurement.* Chichester, UK: Wiley.

The four principles that follow provide practical support for this overarching principle across the varied ways data is managed and used.

Protect individual and collective rights and interests

Individual and collective rights, benefits and interests are often affected by how data is managed and used, either from direct harms or from a failure to create benefits. Protections afforded to these rights and interests by any data governance system must be meaningful and effective.

Data collection, sharing and processing can result in both tangible and intangible harms to individuals, to groups, and to collective interests. Failures in safety-critical systems that rely on datasets, and the socio-technical systems that collect and process data, can endanger individual health, safety and the environment. Non-safety-critical systems can also have adverse consequences, particularly if they rely on datasets that introduce or entrench problematic social biases,[99] or unfairly exclude individuals from opportunities or services.[100]

Consider collective rights and benefits

Data can empower individuals and communities to exercise rights that they previously found difficult to exercise effectively. These opportunities should be actively pursued.

At the same time, if not given careful consideration, contemporary data practices could pose risks to collective goods and benefits. This could be compared to society's inheritance of the unintended environmental impacts associated with the first industrial revolution, which were not anticipated by early industrialists. Effective data governance therefore requires attention to the ways collective goods may be adversely affected by data management and data use. For example, notions such as privacy should be thought of as both a private good and a collective good.

99 Custers B, Calders T, Schermer B, Zarsky T (eds). 2012 *Discrimination and Privacy in the Information Society.* Heidelberg: Springer. See http://dx.doi.org/doi:10.1007/978-3-642-30487-3 (accessed 10 June 2017).

100 Bowker G, Starr SL. 1999 *Sorting things out: Classification and its consequences.* Cambridge, MA: MIT Press.

Provide meaningful and effective protection

Misuse of data or ineffective governance can lead to both tangible and intangible harms.

Tangible harms can include detriment to health, financial loss or discriminatory treatment.[101] Intangible harms could arise as a result of exclusion from services, facilities or opportunities, or the fear that personally identifiable data may fall into the hands of those who exploit it unfairly. Although these harms are often difficult to detect and to quantify, they are nevertheless real, and often the cause of substantial distress and anxiety.

Data governance regimes must ensure that they provide protection against all harm in a way that is meaningful and effective across varied demographic groups. They must also provide effective redress if harm occurs, rather than making nominal provisions or putting measures in place that cannot be meaningfully enforced in practice.

Effective protection requires careful monitoring and evaluation of the processes and outcomes of data-enabled systems in situations where harm may occur. For example, this may include questions about the balance of responsibility between organisations and individuals when it comes to assessing risks associated with data collection, use and processing.

Ensure that trade-offs affected by data management and data use are made transparently, accountably and inclusively

As demonstrated by the tensions identified in this review, data management and data use are likely to entail complex, contestable and context-dependent dilemmas and trade-offs between competing values and interests.

Effective data governance needs to identify these values and interests. It should seek to achieve balance between them in a way that ensures that the benefits of how data is managed and used can be reaped while its associated risks are managed to a socially acceptable level.

101 For example, the submission from Nuffield Council on Bioethics to British Academy and the Royal Society. 2016 *Data Governance: Call for Evidence*. See https://royalsociety.org/~/media/policy/projects/data-governance/data-governance-call-collated-evidence.pdf (accessed 10 June 2017).

Transparency and accountability

As discussed in the previous chapter, data governance requires negotiation of a series of tensions, balancing competing benefits, risks and interests. If these trade-offs are to be transparent, then the choices involved should allow all those affected to have real and effective opportunities to participate.

Transparency on its own is not sufficient.[102] It is not the same as accountability, nor does it assure it. Accountability is a broader, context-specific concept that can be aided by transparency. It also involves establishing forums where data collectors and users can explain their actions, field questions and, if necessary, take responsibility for the consequences of their action.

Data governance must consider whether adequate accountability mechanisms are in place in particular circumstances. It must endeavour to enable those affected by the data system to use the system so that data management, data use and data users can be held to account.

Participation

Data governance systems need to involve thorough and genuine multi-stakeholder participation.

This requires multi-stakeholder approaches to governance that explicitly, creatively and collectively establish who might be affected by the system in question, and how to encourage them to participate. If feasible, this process should be reiterated, as more views and perspectives accumulate.[103]

These views and perspectives should be diverse across demographics, and also across disciplines, geographies and occupations, where possible. When the societal stakes are high, with large uncertainties and competing values, calling on experts to point us in the right direction is not enough. Instead, a system of governance needs to construct workable and legitimate knowledge from many different viewpoints, methods and experiences.[104]

102 O'Neill O. 2006 Transparency and the ethics of communication. In Heald D and Hood C (eds.) Transparency: The key to better governance? *Proceedings of the British Academy* (135). Oxford: Oxford University Press.

103 Bryson JM. 2004 What to do when stakeholders matter. *Public Management Review*, 6, 1. See http://www.tandfonline.com/doi/abs/10.1080/14719030410001675722 (accessed 10 June 2017).

104 This is often referred to as 'post-normal science'. See Funtowicz S, Ravetz J. 1993 Science for the post-normal age. *Futures*, 31, 7.

Seek out good practices and learn from success and failure

Effective data governance should display a commitment to promoting good practice and embedding continuous learning as a way of improving practices and standards.

Share good practice

Where good practices in data governance are expected to lead to good outcomes, this should be treated as a hypothesis to be evaluated and tested, collaboratively and publicly where possible. Information should be shared about the effectiveness of these data governance practices, as this will expand opportunities for monitoring and spreading best practice.

Learn from failure

In some cases, what constitutes 'good practice' may not be the subject of widespread consensus, particularly when values are in conflict.

This conflict should be welcomed, not be sidestepped. Although it may be culturally challenging to do so, those involved in governance practices should acknowledge failures where they occur. They should be enabled to do so in a way that balances demands for accountability and redress with the importance of learning from these failures.

These behaviours will be especially important in the context of data-enabled systems that are increasingly probabilistic in nature: if systems will perform poorly a certain fraction of the time and software bugs are inevitable, seeking perfection might be futile. Continual improvement, however, remains desirable.

Recognise context

Good practices need to be actively built, maintained and adapted. Those that hold strong in one context may fail in another, or become more or less effective as time passes and technologies and societies change. For example, as new methods of reidentifying previously anonymised data appear, practices of de-identification must be carefully reviewed.

Furthermore, organisations involved in data governance must be aware that 'good practices' bring with them assumptions about what to value, and technologies should be regularly aired and explored to keep up to date and maintain alignment with broader societal views and goals. This is a difficult but necessary task, particularly if stakeholders are reluctant to invest in updating their compliance as requirements change.

Enhance existing democratic governance

Ensuring governance systems of accountability and transparency

Effective data management and data use should support democratic processes, help enact democratic decisions and be subject to democratic oversight.

Governance mechanisms should be built to seek out points where they can connect with democratic systems in ways that are not limited to statute requirements and that may need to be creative and context appropriate to be successful. Alternative chains of accountability should also be explicitly recognised, noting the role of different actors in changing, extending or retracting formal or informal rules.

Ensure proportionality in data management and data use

Proportionality involves some idea of balancing competing interests and objectives, the appropriate relationship between means and ends, as well as a commitment to consistency. There should be a reasonable relationship between the aims of a regulatory regime and the means to achieve these aims. This could include, for example, appropriate enforcement powers or sufficient resources.

4 Essential functions and stewardship

While it would be both impossible and undesirable to try to centralise data governance, there is a clear case for a single body to provide effective stewardship of the data governance landscape. Such a body would support existing arrangements and, where necessary, carry out essential functions in conducting inclusive dialogue, anticipating changes and connecting practices across the governance landscape.

4.1 Essential data governance functions

There are three broad categories of functions that a governance framework for any complex social and technological system undergoing rapid evolution needs to perform:

- **A**nticipate, monitor and evaluate: considering alternative futures, managing risks, keeping pace with changes, and reflecting on performance.

- **B**uild practices and set standards: enabling and continuously improving well-founded practices that can be spread quickly across relevant sectors and uses.

- **C**larify, enforce and remedy: ensuring sufficient arrangements for evidence gathering, debate and decision-making, and for action in the forms of incentives, permissions, remedies for harm, incentives and penalties.

Proper application of the Principles for Data Governance to these functions makes it clear that meaningful stakeholder engagement is essential in developing and conducting all of these functions.

Today, these functions are carried out by a wide variety of public, private and civil society actors. These include the Information Commissioner's Office (ICO), the UK Statistics Authority, research funding agencies, non-governmental organisations (NGO), universities, the judiciary, industry bodies and professional societies. Some actors are sectoral, such as in the National Data Guardian's role with respect to data in medical uses, while others such as the ICO work across sectors. Governance in the UK is, of course, also considerably informed by international frameworks. A review of some of the key legislations in the UK landscape is published alongside this report.[105]

This variety reflects the multiple organisations and individuals involved, the complexity and range of types of data, and implications for the ways it is managed and used. It would be not only impossible but also counterproductive to try to centralise them in any significant way: without a rich and partially overlapping landscape, it seems likely that some functions would be performed narrowly or incompletely, and the overall collective resilience and adaptability would be diminished.

105 British Academy and the Royal Society. 2017 *Data Governance: Landscape Review.* London: The Royal Society.

However, this variety also raises questions about collective stewardship of the overall governance landscape. As a result, we believe there is a clear gap for a new body charged with stewardship of the whole landscape, rather than being directly responsible for implementation within specific domains.

The purpose of such a stewardship body would be to support delivery of the full breadth of critical functions in accordance with the Principles for Data Governance, but it would not entail formal regulatory and enforcement power. We expect that such a body would primarily recommend actions to others, but it may also need the capacity to carry out some functions itself if they could not be performed elsewhere, being careful not to duplicate existing efforts.

In particular, and as a matter of urgency, this stewardship body should conduct inclusive dialogue and expert investigation into the most pressing of the questions and issues identified in this report. It should enable new ways to anticipate the future consequences of today's decisions with a view to informing debate and decisions.

In the sections that follow, we set out the functions of the **data governance landscape as a whole** in greater detail. As noted above, it is right that these functions should be carried out by a range of diverse actors across and within sectors. The specific role and characteristics of a new stewardship body will be considered in section 4.2.

Anticipate, monitor and evaluate

Anticipation, monitoring and evaluation are needed to understand if current governance approaches are effective and to provide insights into how they might need to adapt to the future.

In some areas – for example autonomous vehicles, precision farming or additive manufacturing – it is not possible to know exactly what shape future data governance should take. However, there remains a need to ask meaningful questions because actions taken today will have long-term and cumulative effects. Governance cannot afford to operate in a purely reactive mode. Issues that arise in one area might indicate other problems to come, and practices that emerge in one sector might be of use in another.

Scrutinise the status quo

With many parts of today's governance landscape in tension or under strain, the ability to scrutinise existing and emerging governance mechanisms – whether in the form of legislation, regulatory bodies, voluntary initiatives or professional codes – from a number of angles is a key function of the landscape as a whole.

At a minimum, this should be to ensure that such mechanisms (whether legal, ethical or technical) are aligned with legislative and regulatory frameworks, standards and public opinion. For more mature or consequential interventions, this scrutiny might also consist of monitoring, or supporting the monitoring of, their impact and effectiveness, and considering process, outcomes and future sustainability.

Scan the horizon

Exploration of alternative futures and horizon-scanning can provide insights into events and changes perceived to be of high probability, as well as examples of much rarer 'wild card' events. Sometimes, the most important horizon is to consider long-term futures; in other cases, it is to lay out many medium-term scenarios. Thinking of the future not in simple terms of trends, but more accurately as a dynamic, interwoven series of expected and unexpected events, can help design action plans that better establish flexible, adaptable and resilient governance systems.

Horizon-scanning activities can act as early warning systems, enabling priorities and resources to be shifted, and helping to creatively define and understand emerging concepts or challenges.[106] Tangible activities for horizon scanning include proactive listening and evidence gathering, and staying in touch with potentially disruptive areas of research and practice. Organisations able to undertake this function well must have the capacity to identify and explore potential futures around specific issues to help identify questions, manage risk or enable well-founded public debate.

Set the agendas

Horizon scanning, monitoring and evaluation are in vain without robust mechanisms to ensure that their results shape agendas for further debate and decision. There is no simple recipe for this, but there is a range of factors that might facilitate it.

106 Amanatidou E et al. 2012 On concepts and methods in horizon scanning: Lessons from initiating policy dialogues on emerging issues. *Science and Public Policy* **39**, 2. See https://academic.oup.com/spp/article-abstract/39/2/208/1619090/On-concepts-and-methods-in-horizon-scanning?redirectedFrom=fulltext (accessed 10 June 2017).

First, existing decisions, such as new data-related regulation or voluntary standards, should be encouraged to be adaptive in design. This involves making prior commitments to subject them to re-evaluation at a particular trigger point, and then mobilising new factual information from organisations undertaking anticipation, monitoring and evaluation functions.[107]

Second, it requires the flexibility and resources to change political environments in a timely manner and, where possible, ensure that the richest evidence or analysis is available to decision-makers when it is most needed.

Build practices and set standards

Standards facilitate the spread of well-founded practices across sectors and help to ensure that tasks or governance requirements are performed in a way that minimises additional burdens. Therefore, an important role for a governance landscape is to set standards to help coordinate activities across sectors.

Build evidence-based good practices

Good practices emerge as a result of those who dedicate their creativity, time and effort to envisage them, pilot them and scale them up. A data governance landscape should provide the infrastructure and resources to allow for this kind of experimentation, testing and evaluation without fear of reprisal.

Develop open sociotechnical standards

Standards and certification processes are an increasingly prevalent form of ex-ante governance. It seems increasingly likely that different aspects of the management and use of data will be governed by some form of standardisation process. For example, the GDPR makes explicit, albeit general, provisions for certification, codes of conducts and kite marks focusing on privacy issues and encouraging public sector roles in accreditation or compliance.[108] However, such certification approaches also have their limitations.

There is a range of approaches to developing open standards. Some standards are established by bodies that convene for the purpose of building new standards, such as the British Standards Institution (BSI), International Organization for

107 See McCray LE, Oye KA, Petersen AC. 2010 Planned adaptation in risk regulation: An initial survey of US environmental, health, and safety regulation. *Technological Forecasting and Social Change*. 77, 6. See http://dx.doi.org/doi:10.1016/j.techfore.2009.12.001 (accessed 10 June 2017).

108 Rodrigues R et al. 2016 The future of privacy certification in Europe: An exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology*. 30, 3. See http://www.tandfonline.com/doi/full/10.1080/13600869.2016.1189737 (accessed 10 June 2017).

Standardization (ISO) or World Wide Web Consortium (W3C). Standards in other areas, particularly those focused on ethical considerations and complex global supply chains, are often built as a result of the efforts of non-profit organisations that bring retailers, manufacturers and other interests to a negotiating table (see Perspective 7: Connected approach to standards development). This approach may involve setting up independent international secretariats to manage development, roll-out and audit. Examples of these include the Marine Stewardship Council (MSC) or the Forest Stewardship Council (FSC).

Perspective 7
Connected approach to standards development

Joss Langford is the co-founder of Coelition, a not-for-profit group that supports the responsible use of behavioural data by organisations looking to grow brands and drive social change.

Joss Langford sets out the context, advantages and process of developing open standards.

The ability to use standardised approaches to solve engineering problems is fundamental to the advancement of technology and the dissemination of knowledge. In addition to being faster and cheaper to implement, a solution that has been tested and iterated repeatedly in the field will be safer, present fewer technical risks and have fewer unintended consequences.

Standards can evolve from collective common practice , be promoted from a proprietary source or result from a deliberate, collaborative effort to create a specification with universal appeal. The international, national and industry-specific standards bodies that develop these specifications have proliferated over the last 100 years.

Digital technologies and the arising need for interoperable data management tools have seen the conception of open standards. These standards are available on a fair, reasonable and non-discriminatory basis and are often free of any licensing costs. The bodies that support their development are typically non-government, non-profit and support the successful pooling of intellectual property from commercial organisations.

When creating services in an entirely new sector, businesses must recognise the balance between building the overall market and creating a defendable position within that market. Open standards provide an effective route to convert internal thought leadership into a visible commitment to a community, while also creating

practical tools for cooperation with suppliers and customers. Specifically in the management of personally identifiable data, using open standards is a signal of virtue to the individuals whose data is being processed and a mechanism to fulfil regulatory requirements for data portability.

In our work to progress best practice in the responsible management of dynamic personally identifiable data, Coelition has found the collaborative environment of an open standards process to be both focused and fast moving. We have been able to support the standardisation of data formats, data exchange interfaces and a complete taxonomy of human behaviour events.

The discipline of standards development brings attention to what can be readily implemented by an engineer without ambiguity and how that implementation can be audited with the same clarity. These strict aspects of the standard are known as the normative elements which are subject to compliance statements. Although our work sits within a regulatory context, we do not directly refer to law in these compliance statements. Our challenge has been to create common technical requirements from the full diversity of global privacy regulation that give the best prospects for compliance of an implementation in any single jurisdiction.

An open standard specification also provides the opportunity to publish informative (non-normative) sections. For example, Coelition references these informative elements within membership agreements alongside normative compliance to allow organisations to demonstrate a full privacy-by-design system to their customers.

Clarify, enforce and remedy

In addition to the functions relating to information discovery and dissemination discussed above, different entities in a data governance landscape must have the power to make decisions of varying legal and practical effect. In some cases, these powers may relate to clarification, for example, in the interpretation of guidance or of legal and regulatory frameworks that attempt to be technology neutral. In others, the ability to determine or enforce appropriate forms of remedy will be critical and must include effective redress and compensation. These will be essential in achieving some policy objectives and avoiding or rectifying harm.

Create and strengthen mechanisms of enforcement

Enforcement is an important prerequisite for credible data governance, but its practical form can differ widely and can be sector specific. It might include legally enshrined powers to:

- demand more information
- issue orders for organisations to desist or change their action
- conduct planned and spot assessments
- issue penalty notices
- start prosecutions.

Practical enforcement can also exist with limited specific legal backing. This could include:

- keeping central and visible records to penalise bad performance through bad publicity
- awarding or withholding certification against a given standard using voluntary audit mechanisms.[109]

Technical enforcement systems are promising in some clear-cut cases and can play a role in data governance. For example, it is possible to create software systems that, given the information flows permitted, are incapable of revealing particular information. Statistical approaches based on differential privacy allow an untrusted party to query a dataset for aggregated information without being able to use that information to identify individuals. The cryptographic methods for decentralised calculations described in Box 6: Technology governance also fall into this category.

These technologies play an important role in ensuring that the functions of data governance are carried out, and should be promoted and used where suitable. However, they are no panacea. In particular, where the challenges are complex and there are competing values, these technological solutions can shut down discussion, 'build in' certain values over others, or confuse a complex and contextual notion like privacy for something simpler, like information disclosure.

109 Hybrid approaches are also commonly seen. In media regulation of online streaming technologies, Ofcom manage a list of on-demand video services and companies that fall under section 368A of the Communications Act 2003 and are subject to the Act's provisions. See: Ofcom. 2016 *Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services (ODPS).* See https://www.ofcom.org.uk/__data/assets/pdf_file/0023/39173/a2.pdf (accessed 10 June 2017).

Box 5: Making the most of technology governance

In some cases, data can be governed using mathematical and statistical systems that determine what it is possible to do with it, taking out much of the need for manual audits. As Larry Lessig has argued, in some cases, 'code is law'.[110]

Smart meters serve as an example of where this was possible, but has been taken up to varying extents by different countries.[111]

Smart meters can transmit real-time electricity consumption, from which a wide array of private information can also be inferred with high confidence, such as which television channels you watch, or if you have a burglar alarm. Technological solutions utilising cryptography could help prevent, if preferred, this by allowing energy providers and grid operators to do billing and analytics accurately but remotely, without collecting and centralising all the data or knowing anybody's individual records.

In the UK's smart meter roll-out to all homes and businesses by 2020, these technologies were deemed 'immature' and insufficiently explored. Some found this to be linked to both the way the parameters of the procurement process were set too early on without adequate openness, foresight and scientific engagement, and a lack of innovative expertise of this type within energy providers.[112]

The centralised way in which the UK system is set up would make the deployment of these technologies in the future extremely difficult, while in Germany, the system was amended before roll-out so that these technologies could be taken up in the future.

110 Lessig L. 1999 *Code and Other Laws of Cyberspace.* New York: Basic Books.

111 This is set out in greater detail in the British Academy and the Royal Society. 2017 *Data Governance: Case studies.* London: The Royal Society.

112 See for example Brown I. 2014 Britain's smart meter programme: A case study in privacy by design. *International Review of Law, Computers & Technology.* 2014; 28(2): 172–84 and Connor PM et al. Policy and regulation for smart grids in the United Kingdom. *Renewable & Sustainable Energy Reviews.* 2014 Dec; 40:269–86.

Another approach to enforcement can be found in amplifying the impact and reach of existing enforcement mechanisms. For example, several pieces of legislation also make reference to the possibility of 'super-complaints', where independent organisations (rather than affected individuals) fast-track issues to regulators. Specific accredited consumer bodies, such as Which? and Citizens Advice are empowered to make 'super-complaints' to regulators, including the Financial Conduct Authority and the Competition and Markets Authority.[113]

Act to provide remedy and redress

Enforcement, clarification and certain types of standards are unhelpful without organisations that have the 'teeth' to back them up. This function is likely to be the least developed within the whole data governance landscape, but nonetheless one of the most important. Where it is possible to do real harm with data, even small or cumulative harms, individuals and groups need access to justice, including legal mechanisms and institutions that can provide appropriate remedies and redress of financial and other natures.

For example, some actors are already empowered to issue fines, and data protection authorities such as the ICO have been given powers in the GDPR to fine organisations in breach of data protection rules of up to 4% of global turnover or 20 million euros, whichever is higher.

Such fines act as strong deterrents, but do little to provide redress for individuals harmed by misuse of data. In terms of monetary redress, large incidents are best suited for judicial avenues, but litigating smaller, more dispersed harms could significantly outweigh the cost for many, particularly those not familiar with the legal system.[114]

It is also important to emphasise non-monetary remedies and redress. The data protection framework provides some of these as rights to stop processing or opt out of automated decision-making.[115] Some of these have been strengthened in the GDPR but remain largely untested. Other rights, such as Freedom of Information law, can also serve as redress for contentious decisions about data management

113 Competition & Markets Authority (CMA). 2015 *What are super-complaints?* London: CMA. See https://www.gov.uk/government/publications/what-are-super-complaints/what-are-super-complaints (accessed 10 June 2017).

114 US remedies for algorithmic harms are unlikely to translate cleanly to UK contexts. Small claims courts, particularly in the context of the digitisation of the UK court system, might provide useful forums to experiment with how to deal with evidence of relatively small data-related grievances. Such monetary redress might not even take judicial form, instead drawing on inspiration from areas such as cybersecurity insurance.

115 The articles on automated decision-making both in the Data Protection Act and the GDPR, while using the world 'right', have been interpreted by some countries and courts not as rights but as prohibitions. A lack of case law means their status remains unclear.

and use, particularly of the non-personal variety. However, unlike data protection, this only extends to public decision-making. See also Perspective: Widening access to data to protect against harms which considers how to address harm beyond legislative and regulatory frameworks.

The many unanswered questions and gaps in the remedy and redress landscape are compounded by the fact that new models of liability may be required in light of new autonomous intelligent systems.[116]

Perspective 8
Widening access to data to protect against harms

Roger Taylor is the Chair of the RSA (Royal Society for the encouragement of Arts, Manufacturers and Commerce) Open Public Services Network.

Roger Taylor argues that harms arise from poorly executed processing of data, and that we need access to data-driven systems by researchers equipped to rigorously investigate benefits and harms.

The arrival of ubiquitous computing, continuous data collection and automated decision-making has prompted much discussion about appropriate regulatory actions. The most obvious regulatory tool to use is data protection legislation affording individuals control over how their data is used through consent requirements and improved standards of data security.

However, these mechanisms are limited. Even if security were perfect and consent agreements so well designed that I could exercise effective control over the 'use' or 'purpose' of any processing of my data, I would still have inadequate protection against harms. This is because, in the main, the harms people fear from data use and the benefits they seek cannot be distinguished by reference to 'use'. More often than not, harm is nothing more than poorly executed processing of data for purposes that would be beneficial if done well.

People want data to be used to target information more effectively. They do not want it used for nuisance marketing. This cannot be effectively policed by control of usage of data because nuisance marketing is no more than the poor execution of targeted marketing. In the same way, the use of data for, say, medical diagnosis is considered harmful or beneficial, not according to its use, but according to the accuracy with which it is used.

116 This is discussed in the Royal Society. 2017 *Machine learning: the power and promise of machines that learn by example*. London: The Royal Society. See https://royalsociety.org/topics-policy/projects/machine-learning (accessed 10 June 2017).

As automated data-driven decision-making becomes the norm, we need to focus less on protection from unauthorised use of data and focus more on the quality of execution of data usage for approved purposes. There are a few key points to note in this regard.

First, oversight of the standards to which organisations operate is a useful regulatory tool, but even well-established industries with long-standing systems of regulation (such as auto manufacturing, healthcare or pharmaceuticals) are capable of producing harmful products and services. It is the quality of the product or service that counts.

Second, the quality of data-driven decision-making services cannot be judged from looking at the way data is used for any one individual. It can only be judged by examining how data is used across a whole population. It requires an understanding of the degree to which data used to categorise people according to predicted characteristics and propensities is generating false positives and false negatives.

Third, the complexity of the data used for data-driven decision-making allows for a wide range of potential interpretations. In this environment, the adoption of fixed-quality metrics will generate significant efforts to evade such standards. Given that those being regulated have the advantage in terms of access to data, they are likely to be successful in these endeavours.

In the long term, effective protection against harm is likely to be achieved only by ensuring plural scientific access to data used in such systems. The data should be used to test competing hypotheses about the degree to which they are benefitting or harming individuals. This approach has the advantage of also generating a level of understanding and knowledge likely to maximise the potential benefit from data usage. However, work is needed to square such data access rights against commercial rights of data ownership and to ensure that they do not lead to increased risks of unauthorised data access.

Together these functions make up the full governance landscape and need to be underpinned by stakeholder engagement. This will ground them into the development and conduct of all the functions, supported by access to the necessary skills.[117]

Engagement as a mode of operation

The three broad categories of functions described above constitute the critical functions that are required across the entire data governance landscape. For these functions to be achieved successfully, they must be grounded in engagement.

Such engagement needs to: include activities that consider the context-specific nature of data management and data use; seek thorough and representative viewpoints; and engage deeply with the difficult social and technical issues that sit at the heart of these challenges. This engagement should:

- be a dialogue rather than a one-way activity
- be open
- have a demonstrable capacity to influence policy
- explicitly articulate the competing values at stake, and include evidence as part of discussions of future scenarios.

To be fully effective, the dialogue will need to be widely visible, so that even those who are not interested in being personally involved are able to see it happening. Activities are likely to include structured events or workshops, digital forms of engagement, and use of mixed media engagement channels, including low-tech and no-tech ones. A wide range of bodies already specialise in engaging the public and other stakeholder groups around the societal challenges of technologies,[118] while non-profit organisations work to lobby for and organise the deployment of data technologies within the context of particular social issues, such as openness, privacy and digital rights.[119]

117 This is likely to require actions that target immediate needs, as well as long-term strategies to strengthen capacity at all levels. See for example: The Royal Society 2017. *Machine learning: the power and promise of machines that learn*. London: The Royal Society; Professor Sir Charles Bean. 2016 *Independent review of UK economic statistics*. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/507081/2904936_Bean_Review_Web_Accessible.pdf (accessed 10 June 2017); and Government Transformation Strategy, https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy (accessed 10 June 2017).

118 These include universities, public broadcasters, and general scientific engagement organisations like Sciencewise, the British Science Association, the Royal Institution and the Cheltenham Science Festival.

119 Organisations of this type include the Open Rights Group, the Open Data Institute, Privacy International, the Electronic Frontier Foundation, mySociety and DataKind.

Perspective 9
The importance of public dialogue

Nicola Perrin is currently leading the Understanding Patient Data Taskforce, based at Wellcome, set up in response to the Caldicott Review of data security, consent and opt-outs.

Nicola Perrin considers the NHS care.data fiasco, and explains how trust in data use can easily be lost. Engagement might improve trust if it is done well, but damage it if wexecuted poorly.

The launch of the NHS care.data programme in 2014 was a fiasco. The aim was to collect patient-level data from GP practices across England, and to link this data with information from hospitals, registries and prescribing databases in order to provide better care, inform commissioning and advance research. A worthwhile ambition but, in the face of considerable criticism, care.data was paused after a month and finally abandoned two years later.

The project failed for two main reasons: the communication strategy was extremely poor; and the governance processes were found to be weak. The failure of care. data shows how essential it is to develop a trustworthy system to ensure appropriate use of data, and to engage more effectively with the public to build confidence in that system.

A number of studies have explored how people feel about the increasing use of data within the health sector and beyond. The results are fairly consistent: people are generally supportive of the use of data for research, provided there is a clear public benefit. Studies also suggest that the more information people have, the more comfortable they are with wider uses of data. However, there is a caveat: giving only a small amount of information may actually raise concerns. Very few people currently feel they know how data is used, and having too little information leaves them with unanswered questions. It is only by being provided with further information about the benefits and the safeguards that people become more reassured.

The challenge is how to reach that position without using the time of a four-day citizen jury, or a four-hour focus group. We need to get much better at talking about broader issues surrounding the use of data. It is important to talk about the ‘why’, the benefits of using data, and the safeguards that are essential to protect privacy. There also needs to be more transparency: everyone should be able to find out about how data is used, why and by whom. Understanding Patient Data, a new initiative to support better conversations about uses of health information, has been set up to help achieve this in relation to health. As a starting point, we

have been looking at the vocabulary used to talk about data. The language used is often complex and confusing, but is important to explain technical concepts in an accessible and accurate way, avoiding unnecessary jargon that can be a barrier to understanding.

A single conversation will not be enough. Data-driven technologies are moving rapidly. While new approaches, such as machine learning, offer exciting potential to help clinicians, provide benefits to patients and transform healthcare, they may also raise ethical and social issues that must be clearly addressed. As with the introduction of other emerging technologies, whether genetic modification of crops, stem cells or genome editing, it is important to include the public in meaningful dialogue from an early stage. We need to ensure an ongoing conversation with the public, patients and clinicians, to build confidence that data is being used for public benefit and in a responsible way, with trustworthy governance processes.

4.2 Ensuring effective stewardship through the creation of a new body

Despite the range of actors already carrying out some of these important governance functions in their specific sectors or domains, there is a clear need for a new body to steward the landscape as a whole, rather than being directly responsible for implementation within specific domains.

An effective steward should have a helicopter view of the whole governance landscape, and a vision – grounded in evidence, dialogue and wider societal principles – of how this landscape could improve. The stewardship body should: support delivery of the full breath of essential functions in accordance with the Data Governance Principles;[120] be empowered, whether formally or informally (see section 4.3 Options and models for stewardship), to catalyse existing actors to fill gaps that emerge or are found; and, where that is not possible, act in their absence while sustainable systems are sought. **In particular, it would be expected to conduct inclusive dialogue and expert investigation into novel questions and issues, and to enable new forms of anticipation about the future consequences of today's decisions.**

The stewardship body is not envisioned to have any regulatory functions and care should be taken not to duplicate any existing efforts. Table 1 shows how a stewardship role could initially work in relation to the governance functions described and to the actors currently carrying these out.

Within sectors: sector-specialists would be expected to take a leading role. The stewardship body would provide support in linking their application-specific governance to broader frameworks and wider relevant actors, ensuring that learning spreads across different sectors as quickly and effectively as possible. Where sector-specific gaps are identified, the stewardship body should address these gaps and catalyse actions to fill them.

Across sectors: the stewardship body should support existing bodies responsible for delivering well-functioning cross-sector approaches, such as the ICO. In some areas – for example broad futures, dialogue activity and investigation into novel questions – a stewardship body could take the national lead, and may even wish to consider international collaboration.

120 Application of the Data Governance Principles can also usefully draw from other frameworks and models in the current data governance landscape such as the Cabinet Office's Data Science Ethical Framework, the National Statistician's Data Ethics Advisory Committee and the National Data Guardian.

Table 1: Initial roles that a stewardship body could be expected to perform in relation to other governance actors, such as regulators, standards organisations or industry bodies.

	Anticipate, monitor, evaluate	Build practices, set standards	Clarify, enforce and remedy
Across sectors	The stewardship body could: ▪ support existing cross-sector approaches ▪ take significant independent lead in instances where such approaches are not already present ▪ carry out functions if they could not be performed elsewhere.	The stewardship body could: ▪ support existing cross-sector approaches ▪ take significant independent lead in instances where such approaches are not already present ▪ carry out functions if they could not be performed elsewhere.	The stewardship body could: ▪ support governance actors where they exist.
Within sectors	The stewardship body could: ▪ support governance actors where they exist ▪ take the lead to address any gaps in governance.	The stewardship body could: ▪ support governance actors where they exist ▪ take the lead to address any gaps in governance.	The stewardship body could: ▪ support governance actors where they exist.

The core characteristics of a new stewardship body

In this report, we do not make specific recommendations about the location or funding of the stewardship body, although we remain content to explore and advise on detailed options. However, we are clear about the key requirements that any arrangement must satisfy and, in the section that follows, we detail a series of necessary **characteristics**.

Drawing on experience in other sectors, and applying the Principles for Data Governance to the stewardship body itself, we recommend that it have the following characteristics:

- **Independent** from industry, civil society, academia, and government, to develop and maintain a reputation as a trusted voice on issues of contention and controversy.

- **Deeply connected to diverse communities**, to create dialogue with and between publics, industry, civil society, academia and government.

- **Expert across and beyond disciplines**, to draw on the diverse sources of knowledge, ideas and wide range of practitioners to the tackle the daunting unresolved questions raised by the present and future of data governance.

- **Tightly coupled to decision processes,** shaping agendas and implementation, and referred to formally or informally.

- **Durable and visible**, set up with a timeframe long enough to build the needed trust, legitimacy and visibility to maintain broad and lasting confidence.

- **Nationally focused but globally relevant**, to shape thinking on an international level and learn from and adapt world-leading evidence and experience.

The characteristics we specify are ambitious, so establishing them simultaneously, and to high standards of trustworthiness, will take creativity, effort and resolve.

Independence

To develop and maintain a trusted voice, especially on issues of contention and controversy, it is essential that a new stewardship body is truly independent. This requirement will inform the arrangements for the body's accountability, funding and operational structures. It includes independence from specific industrial sectors, civil society and academia, and sufficient insulation from the political cycle. It must be clear from the start that no sectoral interests or objectives are privileged over others.

Deeply connected to diverse communities

Independence does not mean isolation. In order to be effective at steering the landscape, the stewardship body must navigate the tensions between remaining autonomous and being truly and meaningfully embedded within the variety of constituencies it is intended to serve. These range from diverse individuals and communities to civil society organisations, research institutes, small and medium companies and large multi-national industries.

At times some of these interests will conflict, so openness is likely to be a key factor in enabling proximity to action while remaining truly and visibly free from capture by any one group.

Expert across and beyond disciplines

Data issues cross disciplines, sectors and skill sets, and so the stewardship body must do the same. It must be able to call on evidence and insight from all disciplines: researchers from fields such as statistics, human-computer interaction and computer science should be on hand to critically evaluate options from technical standpoints. At the same time, scholars and scientists in fields such as law, anthropology, political science, history and economics, need to work closely with them to help develop and realise desirable options.

A stewardship body will also need to fully engage practitioners, researchers and users across sectors and domains from health to education, transport, retail, finance and environmental services, and more. In its capabilities, the body will therefore need to be at the forefront of deploying and developing new ways of enabling well-founded and multi-stakeholder public debate and engagement. This should include: having expertise in, or the ability expertly to procure, synthesis of expert evidence across disciplines; public dialogue; and insightful framings of potential futures.

Tightly coupled to decision processes

The stewardship body must be tightly coupled to the places where decisions are being taken, for two reasons. Without this coupling, it will not be able to correctly identify and spot the most important opportunities, risks and gaps where it should act, or to identify the most important sources of expertise or players in the wider stakeholder landscape. It also needs to be sufficiently influential that its findings will be listened to and acted on. For example, without formal powers, there is the possibility that it might become, or might be perceived as becoming, interesting but irrelevant. There are many ways of avoiding this outcome, and they need to be designed in from the start. (See Perspective 10: Modes of governance for characteristics of various modes of governance that may achieve this.)

It is also critical that any stewardship body strikes the right balance between being seen as providing authoritative formal advice, but yet sufficiently far removed from regulation as to not discourage industry engagement. By being connected into multiple decision-making processes relating to data that are currently separate, this body should be able to act as a piece of information infrastructure to feed practices and lessons from one context to another in a natural and timely manner.

Durable and visible

To be fully effective, the stewardship body will need to become a trusted and visible part of the governance landscape, to the extent that people are confident of its legitimacy, even if they do not themselves choose to engage with it. Although the stewardship body should have impact from the start, these levels of trust, confidence and awareness will take time to build up. This characteristic favours certain institutional forms over another – for example, it seems unlikely that any body that was put out to periodic tender, or housed in a non-permanent organisation, would be able to project an image of consistency or durability.

Nationally focused but globally relevant

While this would be a body with a UK-specific remit, it should also shape thinking on an international level and learn from world leading evidence and experience. Data moves easily, and resists borders or particular jurisdictions.

Good practices around how to best carry out the functions described in this report will not just be found in the UK, but in the economic and governance systems of partners around the world. A stewardship body should be well placed both to shape the thinking of important actors around the world, including promoting the Principles of Data Governance, as well as to take and to adapt world-leading evidence, wherever it is found.

Perspective 10
Modes of governance

Walter Merricks is currently the chair of IMPRESS, the Independent Monitor for the Press. He has also held a number of senior appointments in legal and public institutions, including the Financial Ombudsman Service and the Human Fertilisation and Embryology Authority.

Walter Merricks considers benefits and characteristics of various modes of governance, such as a statutory authority, not-for-profit models and merging or strengthening existing bodies.

This report proposes that a new body should be brought into being. What options should be considered? What issues might arise?

1. A public body operating at arms length from government and created by legislation?

A statutory body would carry the authority of Parliament, and could be given legal powers to obtain information, to prohibit certain conduct or to carry out specified intrusive activities. Could this body operate successfully without legal powers?
In any event, it is stated government policy that new arm's-length public bodies, whether executive or advisory, will only be set up as a last resort, when consideration of all other delivery mechanisms for the provision of new services or functions has been exhausted. Indeed, government will only seek to retain existing public bodies if they are performing a technical function, or where their activities require political impartiality, or if they need to act independently to establish facts. A public body would need to be sponsored by a government department, and each of the devolved institutions in Scotland, Wales and Northern Ireland would need to be consulted and their interests taken into account.

2. An independent not-for-profit organisation?

As long as this body is not expected to need intrusive legally-backed powers, and does not need a close connection to government, an independent not-for-profit organisation would seem a suitable governance model. Its objects would describe its geographical scope. The body could be incorporated as a community-interest company, a company limited by guarantee, or a charitable incorporated organisation. It could also be established by a deed of trust. Questions to be considered include whether its objects would be charitable and whether it is likely to receive funds from charitable trusts and foundations. How would the first and subsequent members of its governing board be appointed?

3. Linked to and forged out of an existing organisation?
There are existing foundations to which the new body could be linked or by which it could be brought into being and to which it could be accountable. There are substantial advantages in not having to create an entirely new governance model and being able to draw on the infrastructure of an existing body. Provided a satisfactory relationship of common interests can be found, this would be an attractive and flexible solution.

4.3 Options and models for stewardship

We do not make specific recommendations for the models of stewardship, as the details of institutional design are beyond the scope of this report. There is also no equivalent body in the UK,[121] or elsewhere, which the stewardship body can be directly modelled on; what we have in mind draws from a wide range of evidence and examples, but must also reflect the particular opportunities and challenges of today's data issues and the changing ways governance questions are framed in public debate.

The role of any stewardship body and its place in the landscape are likely to change and develop as data-enabled technologies become even more widely adopted and new challenges emerge.

Annex A, lists some of the institutions that might help shape the thinking around models this stewardship body could follow. These are taken from a range of sectors and none of them are an exact fit for the body we outline, but together they map a range of possible elements to serve as a starting point.[122] In addition, it is worth considering that a new body could be independently located or strategically co-located in or between a variety of existing organisations, in order to make most effective use of existing networks, resources and expertise.

121 International initiatives that might be of interest and where lessons can be drawn, include: the Advisory Board on Artificial Intelligence and Human Society, established in May 2016 under the Japanese Minister of State for Science and Technology Policy in order to advance research and development and use of AI technologies, see http://www8.cao.go.jp/cstp/tyousakai/ai/summary/aisociety_en.pdf (accessed 10 June 2017); the French Digital Council, an independent advisory commission that issues independent opinions and recommendations on questions relating to the impact of digital technologies on the economy and society and consults on new legislation or draft regulation, see https://cnnumerique.fr/en/french-digital-council/ (accessed 10 June 2017).

122 This list has been compiled by drawing from engagement with a wide range of stakeholders throughout the project. See Annex D: Evidence and engagement.

The precise form and functions of the new body should be subject to political and public debate, although we are clear that the need to act is urgent.[123] The initial model should also be regarded as likely to evolve over time, reflecting the fact that many aspects of the data governance landscape are going through significant transitions and the requirements of a stewardship function may change in the next months, years and decades.

As such, a body develops and, if it gained the required legitimacy, it might become a potential venue for future statutory functions. The exact nature of these functions, if any emerge, cannot be pre-empted today but might, for example, include information gathering, clarification of quick-moving issues, or public engagement.

There are two key questions to consider in the establishment of a new body:

- **The importance of the stewardship body feeding into the political and decision-making processes**: It might be set up to report to Parliament directly, for example. It might also feed into processes within relevant departments and regulators or other bodies. Depending on the exact arrangement desired, this might or might not require statutory grounding.

- **The importance of the stewardship body having a secure and long-lasting stream of funding**: In the first instance, this may help build the reputation and legitimacy needed in diverse communities to carry out its role effectively. Without secure funding from the start, a stewardship body is unlikely to have the freedoms needed to carry out ambitious functions and to meaningfully steer the landscape in a way that can demonstrate its value.

Funding from government would need to be carefully managed to ensure independence. External funding sources could play a role, although this would make it more challenging to tie into existing decision-making processes in anything other than an informal manner, which would be unlikely to support the legitimacy of this body.

123 Lessons may be learned from initiatives to regulate media. For example, two regulatory initiatives are: the Press Recognition Panel's IMPRESS; and the Independent Press Standards Organisation (IPSO) which was set up by industry after it rejected attempts to establish a press watchdog by Royal Charter. IPSO has come under criticism for protecting the interests of the industry it is intended to regulate, and IMPRESS has met challenges with industry which considers it to be state-sponsored regulation and a threat to freedom of the press.

The changing nature of data management and data use, the evolving technological context, and the shifting meaning of core governance concepts place today's systems for data governance under stress and risk eroding public trust. The impact of these changes is further compounded by their speed and creates new challenges for data governance. This makes a review of the governance landscape both timely and necessary.

It is likely that society is facing a period of particularly disruptive transition in the coming years. In some areas society cannot yet frame meaningful questions around these issues, while nevertheless taking actions that will have long-term and cumulative effects.

It is essential to have a framework that engenders trust and confidence, to give entrepreneurs and decision-makers the confidence to act now, and to realise the potential of new applications in a way that reflects societal preferences. At the same time, data governance is linked intimately to the governance of so much of life that each step is simply another in the journey, where aspiration, action, evidence, reflection and debate will all continue to play essential parts.

Annexes

Annex A

Governance bodies

Body	Definition	Governance	Mechanisms
Information Commissioner's Office (ICO)	The ICO is the UK's non-departmental public body set up to uphold information rights in the public interest. It reports directly to Parliament and is sponsored by the Department for Culture, Media & Sport (DCMS).	The ICO was established following the 1984 Data Protection Act. Today the ICO oversees: Data Protection Act (1998); The Freedom of Information Act; The Privacy and Electronic Communications Regulations (PERC); The Environmental Information Regulations; INSPIRE Regulations; Re-use of Public Sector Information Regulations (RPSI).	There are several tools available for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.
Climate Change Committee (CCC)	The CCC is an independent, statutory body with the purpose to advise the UK Government and Devolved Administrations on emissions targets and report to Parliament on progress made in reducing greenhouse gas emissions and preparing for climate change.	Established under the Climate Change Act 2008.	The CCC's advice on carbon budgets and targets is directly reflected in legislation and the Government's carbon strategy. In advising on setting and meeting carbon budgets, the Committee undertakes detailed sectoral analysis and, as a result, has made a number of key recommendations which are reflected in areas of energy and climate policy.

Body	Definition	Governance	Mechanisms
National Institute for Biological Standards and Control (NIBSC)	NIBSC is a global leader in the characterisation, standardisation and control of biological medicines. It plays a major role in assuring the quality of biological medicines through: developing standards and reference materials; product control testing; carrying out applied research.	In 2009, NIBSC became centre of the UK Health Protection Agency (HPA). In 2013, the NIBSC left the HPA and merged with the UK's Medicines and Healthcare Products Regulatory Agency (MHRA).	NIBSC prepares, evaluates and distributes international biological standards and other biological reference materials, supplying over 90% of these for the World Health Organization (WHO).
Citizens Advice	Citizens Advice is a charity with a variety of public functions that are achieved in partnership with government. Some of these include supporting enforcement functions of consumers in particular sectors, such as in finance, energy and postal services.	The statutory basis for Citizens Advice is laid out in the Financial Services Act 2012.	The Treasury has designated that Citizens Advice can bring complaints levied at a sector rather than an individual firm to the Financial Conduct Authority, who are obliged to respond.
Human Fertilisation and Embryology Authority (HFEA)	HFEA regulates the use of gametes and embryos in fertility treatment and research. It inspects and issues licences to fertility centres and to centres undertaking human embryo research.	HFEA draws statutory functions as a regulator from the Human Fertilisation and Embryology Acts 1990 and 2008.	HFEA's statutory functions include licensing IVF clinics, monitoring research establishments, mainlining registers of licenses and regulating gamete storage. HFEA also has an advisory role.
National Audit Office (NAO)	NAO is a non-parliamentary body, led by the Comptroller and Auditor General (C&AG) that may 'carry out examinations into the economy, efficiency and effectiveness with which any (government department or other relevant body) has used its resources in discharging its functions', in addition to other organisations where public money is spent.	NAO's legal authority arises from the National Audit Act 1983.	NAO's objective is to support Parliament in holding government to account and driving improvement in public services. NAO examines how policy is formulated, and frequently examine aspects of the policy-making process.

Body	Definition	Governance	Mechanisms
Parliamentary and Health Service Ombudsman	The Ombudsman is an independent statutory body. It was established by Parliament to make final decisions on complaints that have not been resolved by the NHS in England, UK government departments and some UK public organisations.	The Ombudsman draws powers primarily from Parliamentary Commissioner Act 1967 and the Health Service Commissioners Act 1993.	The Ombudsman may make recommendations for organisations that can include explanations, apologies and recommendations for the service to learn and improve.
Office for Budget Responsibility (OBR)	OBR is a non-departmental public body established to examine and report on the sustainability of the public finances.	OBR was established under the Budget Responsibility and National Audit Act 2011.	OBR has a right of access to relevant information held by any minister of the Crown or government department, and with this right produces several reports a year as detailed in statute, lays them down before Parliament and sends them to the Treasury.
Better Regulation Executive (BRE)	BRE is an administrative unit within the Department for Business, Energy & Industrial Strategy. It works with government departments to monitor the measurement of regulatory burdens and coordinate their reduction, and to ensure that the regulation that remains is smarter, better targeted and less costly to business.	BRE began in 2010 attached to the Cabinet Office, working and publishing information and advice. Categorised as a Department's Office or Taskforce, it is set up at ministerial discretion, without legislation or separate legal entity.	The Government is implementing a set of policies aimed at improving the way regulation is applied. These include a statutory code of practice for regulators underpinning the Principles of Better Regulation – the Regulators' Code.
National Data Guardian (NDG)	NDG is sponsored by the Department of Health, but operates independently. NDG's role is to help make sure that the public can trust that their confidential information is securely safeguarded and is used to achieve better outcomes from health and care services.	Dame Fiona Caldicott was appointed as the first NDG in 2014. The UK Caldicott Guardian Council is a sub-group of the NDG's panel and the national body for Caldicott Guardians.	NDG currently lacks a statutory footing, although the Department of Health is exploring a range of mechanisms by which it could be achieved, including through relevant primary legislation, by a Statutory Instrument, or by extending the legal remit.

Body	Definition	Governance	Mechanisms
The Charity Commission	The Charity Commission is responsible for: registering eligible organisations in England and Wales; taking enforcement action when there is malpractice or misconduct; ensuring that charities meet their legal requirements; making appropriate information about each registered charity widely available; and providing online services and guidance to charities.	The Charity Commission is established under the Charities Act 2006.	The Charity Commission may use its powers of protection which include: restricting the transactions that a charity may enter into; appointing additional trustees; 'freezing' a charity's bank account; suspending or removing a trustee; and appointing an interim manager.
General Medical Council (GMC)	The GMC helps to protect patients and improve medical education and practice in the UK by setting standards for students and doctors and take action when the standards are not met.	The Medical Act 1858 established the General Council of Medical Education and Registration of the United Kingdom as a statutory body.	Serious or persistent failure to follow professional standards will put a doctor's registration at risk. Following an investigation, the council may issue advice or a warning to the doctor, or may agree with the doctor that they will restrict their practice, retrain or work under supervision. In some cases, they will refer the case to the Medical Practitioners' Tribunal Service.
Local Government Ombudsman	The Local Government Ombudsman is the final stage for complaints about councils and some other organisations providing local public services. The Ombudsman also looks at complaints about adult social care providers.	The Local Government Ombudsman positions were created as a result of the Local Government Act 1974, which was amended by the Local Government and Public Involvement in Health Act 2007.	The Ombudsman may ask a council to reconsider a decision. If that is not possible, they might ask the council to take action to put right the effects of a decision which was not made in the correct way. This might involve a payment.

Body	Definition	Governance	Mechanisms
UK Statistics Authority (UKSA)	The Authority is a non-ministerial, independent statutory body with the objective of promoting and safeguarding the production and publication of official statistics that 'serve the public good'. The National Statistician is the UK Statistics Authority's and Government's principal adviser official statistics, as well as the Head of the Government Statistical Service.	The Statistics and Registration Service Act 2007 established the UKSA. Before 2008, the system was governed by the non-statutory 2000 Framework for National Statistics.	The Code of Practice for Official Statistics has statutory underpinning and statisticians are under an obligation to adhere to its ethical requirements. Compliance with the Code is a statutory requirement on bodies that produce statistics that are designated as National Statistics.

Annex B

Terms of reference

- Identify the communities with interests in the governance of data and its uses, but which may be considering these issues in different contexts and with varied aims and assumptions, in order to facilitate dialogue between these communities. These include academia, industry, the public sector and civil society.

- Clarify where there are connections between different debates, identifying shared issues and common questions, and help to develop a common framework and shared language for debate.

- Identify which social, ethical and governance challenges arise in the context of developments in data use.

- Set out the public interests at stake in governance of data and its uses, and the relationships between them, and how the principles of Responsible Research and Innovation (RRI) apply in the context of data use.

- Make proposals for the UK to establish a sustained and flexible platform for debating issues of data governance, developing consensus about future legal and technical frameworks, and ensuring that learning and good practice spreads as fast as possible.

Annex C

Acknowledgements

Working group

The members of the working group involved in this report are listed below. Members acted in an individual and not a representative capacity, and declared any potential conflicts of interest.

Members contributed to the project on the basis of their own expertise and good judgment.

Regular members

Professor Dame Ottoline Leyser DBE FRS (Co-Chair)	Chair of the Royal Society Science Policy Advisory Group
Professor Genevra Richardson CBE FBA (Co-Chair)	Chair of the British Academy Public Policy Committee
Professor Jon Agar	Professor of Science and Technology Studies, University College London (UCL)
Professor Dame Wendy Hall DBE FREng FRS	Professor of Computer Science at the University of Southampton
Professor Amanda Chessell CBE FREng	IBM Distinguished Engineer Master Inventor
Professor Luciano Floridi	Professor of Philosophy and Ethics of Information and Director of the Digital Ethics Lab, Oxford Internet Institute, University of Oxford; Faculty Fellow and Chair of the Data Ethics Group, The Alan Turing Institute
Professor David Hand OBE FBA	Emeritus Professor of Mathematics, Imperial College London, and Non-Executive Director of the UK Statistics Authority Board
Dr Hannah Knox	Lecturer in Digital Anthropology and Material Culture, UCL
Professor Sofia Olhede	Professor of Statistics at UCL and honorary chair in the UCL computer science department
Mr Antony Walker	Deputy CEO of techUK
Professor Karen Yeung	Professor of Law and Director of the Centre for Technology, Ethics & Law in Society (TELOS), The Dickson Poon School of Law, King's College London; Distinguished Visiting Fellow, Melbourne Law School, Australia

Contributing members

Contributing members provided expert feedback and input throughout the development of the report.

Professor Chris Bishop FREng FRS	Technical Fellow and Laboratory Director of Microsoft Research in Cambridge
Professor Andrew Morris FMedSci	Director of the Usher Institute of Population Health Sciences and Informatics, and Vice-Principal Data Science, University of Edinburgh
Professor Martyn Thomas CBE FREng	Professor of Information Technology, Gresham College

Review panel

This report has been reviewed by an independent panel of experts. The Review Panel members were not asked to endorse the conclusions or recommendations of the report, but to act as independent referees of its technical content and presentation. Panel members acted in a personal and not a representative capacity, and were asked to declare any potential conflicts of interest.

The British Academy and the Royal Society gratefully acknowledge the contribution of the reviewers:

- Baroness Onora O'Neill FRS FBA FMedSci
- Professor Andy Hopper FREng FRS
- Professor Patrick Maxwell FMedSci
- Professor Sir Martin Sweeting FREng FRS
- Ray Shostak CBE
- Professor Sir Ian Diamond FBA

Contributions

The British Academy and the Royal Society would also like to acknowledge the contributions to this report from the following individuals:

- Michael Veale
- Fernanda Ribas
- Marion Oswald

Staff from across the British Academy and the Royal Society contributed to the production of this report.

Dr Claire Craig CBE	Director of Science Policy Royal Society
Dr Natasha McCarthy	Head of Policy – Data Royal Society
Louise Pakseresht	Senior Policy Adviser Royal Society
Jessica Montgomery	Senior Policy Adviser Royal Society
Dr Franck Fourniol	Policy Adviser Royal Society
Susannah Odell	Policy Adviser Royal Society
Dr Clare Dyer	(Former) intern, Royal Society
Will Kay	Intern, Royal Society
Vivienne Hurley	Director of Research Funding and Policy British Academy
Lisa Davis	Head of Policy (Public) British Academy
Barbara Limon	Interim Head of Policy (Public) British Academy
Helen Gibson	Policy and Engagement Manager British Academy
Tara Vernhes	Policy Advisor British Academy

Annex D

Evidence and engagement

This review gathered input from a wide range of sources and the review team are grateful to all who participated and gave their time and expertise.

A call for evidence was issued and submissions were received from the following organisations and individuals:

- Academy of Medical Sciences (AMS)
- Administrative Data Research Centre England (ADRCE)
- Alan Sturt (individual response)
- Association of Medical Research Charities (AMRC)
- Consumer Data Research Centre, UCL
- Genetic Alliance UK
- Information Commissioner's Office (ICO)
- James Denman (personal response)
- medConfidential
- National Data Guardian
- Newcastle University
- Nuffield Council on Bioethics
- Population Data Science, Swansea
- Privacy International
- Royal Statistical Society
- techUK
- UK Statistics Authority
- Wellcome Trust

The British Academy and the Royal Society held a series of events and roundtables between July 2016 and 2017:

Scoping seminar (July 2016)
Around 60 attendees from academia, government and business, including experts in ethics, law, finance, social and data sciences, machine learning and statistics. A seminar report, Connecting debates on the governance of data and its uses, was published, together with 16 provocation papers.

Roundtables

Humanities and social science perspectives on data's collection, management and use (20 October 2016)
Chaired by Professor Jon Agar. Considered governance from the perspective of historians, psychologist and anthropologists.

Advisory roundtables (11 November and 9 December 2016)
Gathered evidence from academies, learned societies, think-tanks and other policy organisations involved in data-related policy work.

Data governance for how we do business (5 December 2016)
Chaired by Dr Mike Lynch FRS, with representatives from Google UK, Facebook, Microsoft and IBM, to discuss governance, digital industry and multinational companies.

Data governance in law (19 January 2017)
Chaired by Professor Karen Yeung. Seeking input from legal expertise on the current governance landscape and the governance needs.

Civil society (23 January 2017)
Chaired by Professor Jon Agar. Brought together representatives from civil society groups to discuss public views, concerns and opportunities relating to data governance.

Governance leaders (31 January 2017)
Chaired by Professor Lord Robert Mair FREng FRS and with Baroness O'Neill, Walter Merricks, Sir Michael Rawlins, Sir David Omand, Sir John Chisholm and Lord Broers participating. Considered the lessons and challenges of large-scale reviews and governing complex issues.

SMEs and start ups jointly with the Digital Catapult (31 January 2017)
Chaired by Professor Neil Lawrence, member of the Royal Society Machine Learning Working Group. Holds discussions to understand governance challenges and opportunities for small and medium-sized businesses in the digital sector.

Glossary

Algorithm: A set of rules a computer follows to solve a problem.

Artificial intelligence: An umbrella term for the science of making machines smart.

Autonomous intelligent systems: Systems, such as cars, that use AI and machine learning technologies to function without a human agent being in direct control and which can use learning techniques to determine courses of action in new contexts

Bias: Selection of data or samples in a way that does not represent the true parameters (or distribution) of the population.

Big data: Large and heterogeneous forms of data that have been collected without strict experimental design. Big data is becoming more common due to the proliferation of digital storage, the greater ease of acquisition of data (e.g. through mobile phones) and the higher degree of interconnection between our devices (i.e. the internet).

Data: Numbers, characters or images that designate an attribute of a phenomenon.

Data exhaust: The data generated by an individual through daily activities.

Filter bubble: The restriction of a user's perspective that can be created by personalised search technologies.

Governance: In this report governance is taken to mean everything that directly informs the extent of confidence in data management, data use and the technologies derived from it. This includes the institutional configuration of legal, ethical, professional and behavioural norms of conduct, conventions and practices that, taken together, govern the collection, storage, use and transfer of data and the institutional mechanisms by and through which those norms are established and enforced.

Machine learning: A set of rules that allows systems to learn directly from examples, data and experience.

Metadata: 'Data about data', contains information about a dataset. For example, this information could include why and how the original data was generated, who created it and when. It may also be technical, describing the original data's structure, licensing terms, and the standards to which it conforms.

Sensitive (data): Sensitivity has strict definitions under the Data Protection Act, but for the purposes of this report it refers to data or information that an individual would not wish to be widely and openly known.

BRITISH ACADEMY
for the humanities and social sciences

The British Academy
10–11 Carlton House Terrace
London SW1Y 5AH
+44 (0)20 7969 5200

Registered Charity:
Number 233176

britishacademy.ac.uk

@britac_news
TheBritishAcademy
britacfilm
BritishAcademy

THE ROYAL SOCIETY

The Royal Society
6–9 Carlton House Terrace
London SW1Y 5AG
+44 20 7451 2500

Registered Charity:
Number 207043

royalsociety.org

@royalsociety
@theroyalsociety
RoyalSociety

Issued: June 2017
Cover image: ©Matjaz Slanic (iStock)
Design by Soapbox, www.soapbox.co.uk