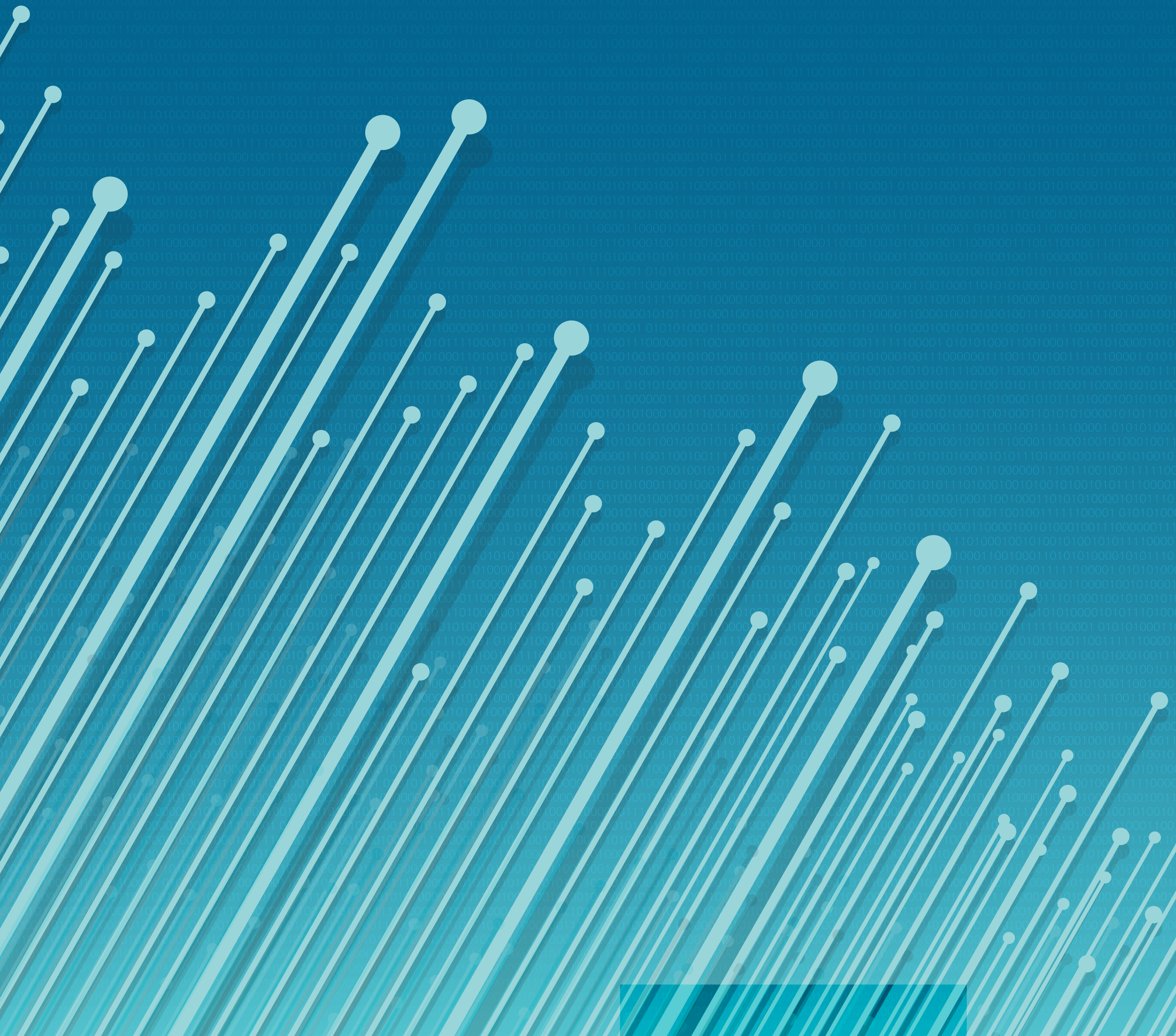
policy connect

All-Party Parliamentary Group on
dataanalytics

BUILDING ETHICAL DATA POLICIES FOR THE PUBLIC GOOD

TRUST, TRANSPARENCY AND TECH



May 2019

This report follows a six month Inquiry and was written by Jack Tindale and Oona Muirhead CBE, Policy Connect.

This Inquiry was kindly supported by Deloitte and Jisc. The views and opinions presented in this report do not necessarily represent those of the supporters.

Policy Connect
7-14 Great Dover Street
London
SE1 4YR

www.policyconnect.org.uk

CONTENTS

Foreword

Data-driven technologies are revolutionising the way important decisions are made every day. From our treatment in hospital to students' educational experience; from how we travel to the way our society is policed; we are increasingly reliant on data to enable modern life. However, these developments have not always been accompanied by openness and accountability about the use of our information. This lack of transparency has led to a growing distrust and suspicion about data and algorithm-based decisions, concerns which must be overcome if we are to exploit the many positive ways that data-based technology can improve people's lives.

The All-Party Parliamentary Group on Data Analytics is clear that these are issues to be tackled now. So, we have resisted the temptation to look into the technological challenges of the far future, but instead have concentrated on the issues that matter today - how to bring decisions about data ethics closer to the people they affect most: the public.

There are some who say data capture and use is out of control, and that the complexity of the technologies it informs and the way algorithm-based decisions are taken are beyond the scope of government influence. We do not agree. Government and Parliament both have leadership roles to play in a new settlement for data governance based on public consent, cooperation and openness: using the power of public procurement and enhancing parliamentarian oversight.

For such a new settlement to start, the government and those organisations providing public services to our constituents need to meet new, consistent standards. And in our mixed economy of public, private and voluntary organisations it is all the more important there should be a single set of principles for all those interacting with the citizen. We are therefore proposing that all such organisations should conform to the highest standards of transparency and engagement as their 'licence to provide public services'. We have built on the latest thinking in relation to freedom of information: that these important issues of openness and accountability to the public should apply to all those delivering services paid for by the taxpayer.

Parliament also has a key role to play in providing challenge and scrutiny, just as it has done in the past in addressing the big societal issues of the time, from public accounts to the environment. A data-driven world is the next major challenge - and opportunity - and parliamentarians should be working now to steer the UK into this future. How parliament engages in the topic, and holds the government, public services and the wider economy to account, will be crucial.

We firmly believe that if parliament, government, industry and the public work together, we can define the acceptable boundaries of data use and thereby achieve greater understanding and acceptance of data in our lives. The UK has the opportunity to seize the agenda and become a world leader in the ethical use of data as a means of innovation in technology and services.

We would like to thank the very committed and engaged group of parliamentarians, industry and civil society experts who have given their time to this Inquiry, as well as Deloitte and Jisc without whose sponsorship it could not have happened. We recognise that these are complex and potentially controversial issues and expect that not all of those engaged will agree with every part of the report. We are, however, clear that if we are to build public trust we need to be open and honest, including about past mistakes.

Lee Rowley,
Conservative Member
of Parliament for North
East Derbyshire

Darren Jones,
Labour Member of
Parliament for Bristol
North West

Recommendations

Public Services ‘Licence to Operate’

Recommendation 1: To build public confidence and acceptability, providers of public services should address ethics as part of their ‘licence to operate’. A core principle should be that the public’s views on data exploitation are proactively built into an ethical assessment at the service design stage.

Recommendation 2: The citizen should be given access to simple and meaningful information, akin to the transparency principles underpinning Freedom of Information. This duty should apply to all those using data exploitation to deliver public services, as part of their ‘licence to provide public services’.

Recommendation 3: The citizen should have a ‘right to explanation’, via a duty on all those delivering public services to provide easy to understand information on the factors taken into account in algorithm-based ‘black-box’ decisions as they affect the individual.

Recommendation 4: There should be clear lines of accountability on data and algorithm use to the top of every organisation providing public services, including accessible complaints and redress processes. This could be achieved by extending the Data Protection Officer role and updating company director responsibilities.

Recommendation 5: To ensure a consistent experience for the citizen, all Departments’ existing governance arrangements should be assessed to ensure they are providing a coherent ethics framework for devolved public service delivery such as NHS trusts and police forces, enforceable through respective regulators. Where necessary independent Data Ethics Advisory Boards should be established, which could link to the UK Artificial Intelligence Council established in the Artificial Intelligence (AI) sector deal and to the Centre for Data Ethics and Innovation.

Centre for Data Ethics and Innovation Workplan

Recommendation 6: The Centre, working with departmental data ethics centres such as the Centre for Connected and Autonomous Vehicles, should address the trust risks that could inhibit innovation:

a. Develop a user-friendly means - such as a kitemark - to show when a decision is taken by machine intelligence, and when you are interacting with a machine not a human, and mandate its use across government and public service delivery in higher risk areas.

b. Provide central guidance on ‘responsible trials’ of Artificial Intelligence technology such as biometrics and facial recognition as well as autonomous vehicles.

c. Develop a way for pedestrians and other road users to identify an autonomous vehicle along the lines of a ‘P’ plate.

Recommendation 7: The Government should prioritise work on ‘consent’ as this is an aspect particularly challenged by data-driven technology, and invite the Centre to carry out a full thematic review into a model for assumed public consent for common good, taking account of lessons learnt. This should consider issues around informed versus implied consent, and how to ensure the consent process is fit for purpose and not a simple tick-box exercise.

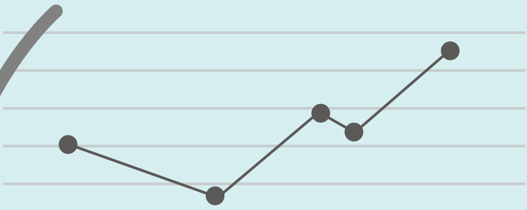
Role of Parliament

Recommendation 8: To enhance parliamentary scrutiny, the legislation to establish the Centre as an independent statutory body should include the requirement for the Centre to submit their proposed annual report to parliament for scrutiny through the current Select Committee process.

Recommendation 9: Parliament should take a greater leadership role in assessing privacy issues and consider the need for an overarching Select Committee given the ever-growing importance for public trust and confidence of the data-driven and technology influenced world.

A BRITISH STRENGTH

The British digital industry is worth £184Bn



Employment grew by 13.2%

2014 - 2017

London is second only to Silicon Valley for inbound global connections

Workers were £10,000 more productive per person per annum

Steps for building public confidence in accountable data and technology roll outs:

- Organisations providing public services should have a license to operate, displaying high standards for how they use and apply data-intensive technology.
- Users that engage with data collection and machine learning should know up front when they are engaging with AI and sharing their data.
- Ensure that meaningful user ethics and consent are built into the design stages of technology, data handling and regulation from the start.
- Establish Parliamentary oversight for the Centre for Data Ethics and Innovation to ensure citizens' rights are protected.

It could help with mental health support and course design in the future

University tutors at the University of Greenwich are using a data dashboard to monitor student progress and improve outcomes for the first time

Students are using the Study Goals app like a fitness tracker for their studies

56%

of disabled people shared their excitement at the prospect of connected & automated vehicles helping them in their daily lives, according to a YouGov poll

94%

Confidence interval

Saving Sight

Data collected by Moorfields Eye Hospital means that artificial intelligence can now diagnose more than 50 sight-threatening conditions

Executive Summary & Key Sectoral Findings

The new Centre for Data Ethics and Innovation (CDEI) was announced in the 2017 Budget to develop the measures needed to strengthen and improve the way data and AI are used. On 20th March 2019 the Centre set out its first two-year strategy and its work programme for 2019/20, its first full year of operation. The strategy focuses on the role of the Centre to help the UK become a global leader in responsible innovation in data-driven technology.

The All-Party Parliamentary Group on Data Analytics (APPGDA) believes that the UK will only achieve this ambition if both government and the private sector build the public's confidence in data and technology. The Group therefore set up this Data and Technology Ethics Inquiry (the "Inquiry") to inform the debate as the Centre develops its remit and scope. It focused in particular on the challenges around building and maintaining public trust and confidence, and the challenges to the ethical application of data and data-driven technology in the UK. It concentrated on the ethical barriers that exist now or will do in the near future, and where we can investigate real-world issues and develop recommendations with real impact. It also considered how to strengthen the parliamentary scrutiny of ethical data use to ensure that the principles behind data protection are upheld.

The Inquiry considered how ethical standards and frameworks can enable innovation and provide a reliable, trusted jurisdiction for both individuals and companies - thereby potentially providing the UK with a commercial advantage.
To ensure that the Inquiry was firmly based in reality and focusing on actual problems of ethics and innovation, it looked at four key areas of our lives: autonomous vehicles, healthcare, education and policing. The Inquiry was therefore able to draw out some comparative experience, problems and solutions, as well as some findings and recommendations specific to each sector, to help ensure the UK follows through on its aspiration to be a global leader in responsible innovation in data-driven technology.

> **One of the greatest individual challenges posed by new information technologies is privacy. We instinctively understand why it is so essential, yet the tracking and sharing of information about us is a crucial part of the new connectivity. Debates about fundamental issues such as the impact on our inner lives of the loss of control over our data will only intensify in the years ahead.[1]**
>
> Klaus Schwab - The Fourth Industrial Revolution: What it Means and How to Respond.

Definitions and assumptions

Despite a considerable rise in the use of terms such as "artificial intelligence" and "machine learning", there is a lack of any real industry standard or international definition of AI. The House of Lords Select Committee noted that this is to be expected, given that there is also a lack of any formal definition of organic intelligence[1]. However, a broad overview of these areas can be made.

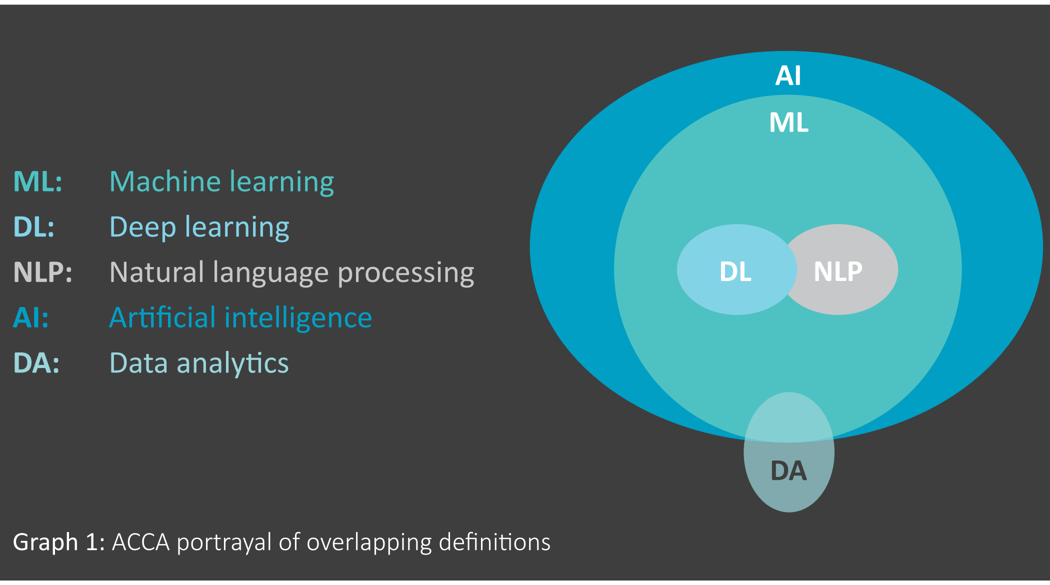
The Department for Business, Energy and Industrial Strategy (BEIS) defines **artificial intelligence** as being "technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation"[2]. This was echoed in a recent report by the Association of Chartered Certified Accountants (ACCA) which described AI as "the ability of machines to exhibit human-like capabilities in areas such as thinking, understanding, reasoning, learning or perception"[3].

[1] House of Lords, AI in the UK: ready, willing and able?, 16th April 2018, pg. 13.
[2] HM Government, Industrial Strategy: Building a Britain fit for the future, November 2017, pg. 37.
[3] ACCA, Machine Learning: More Science than Fiction, April 2019, pgs. 12.

The House of Lords defined **machine learning** as follows:

One particular form of AI, which gives computers the ability to learn from and improve with experience, without being explicitly programmed. When provided with sufficient data, a machine learning algorithm can learn to make predictions or solve problems, such as identifying objects in pictures or winning at particular games[4].

The ACCA study[5] also noted a degree of overlap between machine learning and **data analytics,** with the difference that data analytics is a process that is generally controlled and led by a human actor. The graph below highlights the overarching and interlocking relationship between many of these terms[6]:



Graph 1: ACCA portrayal of overlapping definitions

Another key distinction that needs to be made is between the concept of **Ethics by Design** and **Pro-Ethical Design.** In his role as advisor to the Inquiry, Professor Luciano Floridi noted the practical differences between the two[7], based on a wide volume of research, including an article to the leading journal on technology ethics[8].

Ethics by Design can be paternalistic in ways that constrain the choices of agents - it makes some options less easily available or not at all. In contrast, **pro-ethical design** still forces agents to make choices, but this time the nudge is less paternalistic because it does not preclude a course of action but requires agents to make up their mind about it.

As an example of this - a speed camera is a form of nudging (drivers should respect the speed limits) but it is pro-ethical insofar as it leaves to the drivers the freedom to choose to pay a ticket, for example in case of an emergency. Speed bumps are however a kind of traffic calming measure designed to slow down vehicles and improve safety that motorists cannot avoid. They involve a physical alteration of the road, which is permanent and leaves no real choice to the driver - so represent ethics by design (whether a good idea or not). This means that emergency vehicles, such as a medical ambulance, a police car, or a fire engine, must also slow down, even when responding to an emergency[9].

[4] House of Lords, AI in the UK: ready, willing and able?, 16th April 2018, pg. 14.
[5] ACCA, Machine Learning: More Science than Fiction, April 2019, pg. 12.
[6] Ibid.
[7] Floridi L, Evidence to the Inquiry, 10th April 2019.
[8] Floridi L, Tolerant Paternalism: Pro-ethical Design as a Resolution of the Dilemma of Toleration, Science and Engineering Ethics, December 2016, Volume 22, Issue 6, pgs. 1669–1688.
[9] Floridi L, Evidence to the Inquiry, 10th April 2019.

Connected & Autonomous vehicles

Self-driving vehicles represent a leap forwards from the technology that drivers currently take for granted such as satnavs and parking aids. They offer real social benefits, such as supporting the elderly and disabled to live independently. But there are cultural issues around safety to be overcome (fears have been exacerbated as a result of a death arising in a recent US trial), and significant untangling needs to be done of accountability and liability issues for when things go wrong. Some car manufacturers have announced they will take responsibility for their autonomous vehicles (AV), but what does that mean in practice? Commercial issues around intellectual property currently preclude the interrogation of data, as has been seen in recent inquiries into accidents. Will manufacturers underwrite insurance irrespective of the circumstances surrounding a major motorway pile-up?

Autonomous vehicles also bring forward ethical considerations around personal data collected during journeys, who owns it and how it is stored and exploited. For example, passengers may rightly be sensitive about who has access to data on their regular routes and destinations, and to what use that knowledge is put.

The social acceptability of AV and the implications for social equity are also relevant. For example, in cities the development of automated vehicle technology and its infrastructure could clash with broader transport, health and environmental policies on vehicle use. The Inquiry suggests that, to ensure technology does not take precedence over wider societal benefits, the development of AV infrastructure - at the very least in those major cities promoting walking, cycling and public transport - should be required to support broader place-shaping policies. A possible solution could be to focus AV in cities on buses, trams and trains with a clearer relationship between the automotive sector, transport authorities, and urban planning.

The future ‘rules of the road’ need to take into account the challenges of human-machine interaction. Humans decide their actions in the public realm not just by reference to hard rules of the road but also through soft social interactions such as eye contact and gestures, not possible if one interlocutor is a machine.

The following are key findings from this strand of the Inquiry specific to autonomous vehicles:

- Data ownership of personal data collected by vehicles will need to be carefully addressed, as will public confidence in the robustness of the cyber security approach.
- The capture of personal data from passers-by could lead to loss of privacy in public places.
- Issues around access to the ‘brain’ of the AV need to be addressed, potentially through an accident ‘black-box’.
- It should be very clear to road users when a vehicle is partially or fully controlled by a machine, to ensure humans do not make assumptions about likely vehicle behaviour.

Healthcare

Of the four thematic areas investigated by the Inquiry the role of data in the healthcare system resulted in the most wide-spread discussion and the largest number of individual submissions. The Inquiry acknowledged that data use in healthcare presents enormous opportunities for common good in a number of fields. For example, research has shown that people with dementia have changes in the retina, and a study is being carried out to see if patterns from the data could be used to develop an early detection tool for dementia before patients show signs of cognitive decline.

On public trust, there was a clear sense that there is an inherent social settlement between the public and NHS about data - that it may be used for the purposes of improving both their own and the health of the population at large. However, there have been poorly executed data-based programmes in the past and the Inquiry heard that these have provided a warning that the high level of trust in the NHS should not be taken for granted, and furthermore should not be assumed to extend to the NHS's ability to safeguard data. For example, a 2018 study by the Open Data Institute into British consumer attitudes showed that if the high level of public support for the NHS and confidence in the existing 'implied consent' model is to be retained, more proactive and overt discussions are needed with the public on how and why the NHS uses data, and in the robustness of the NHS's data infrastructure. A distinction could in principle be drawn between aggregated anonymised data and sensitive personal healthcare data, but some participants were concerned that in practice it was not possible for data to be fully anonymised.

Further, respondents drew a distinction between the social contract between patients and doctors that has already allowed large data sets to be captured and analysed, for example in the National Joint Registry[10], and the extension of this 'contract' to the private sector. The absence of oversight to ensure that data provided for one purpose (such as the health of the individual or the public where the outcome is a common good) is not used for another (such as marketing or insurance where the outcome is commercial profit), and blurring of accountability for when data is misused led the Inquiry to conclude that there is a need to reassess the principles of consent for data-sharing, with patients contributing to that reassessment. If the system covering data-sharing is so complex it is impossible to explain it to patients, it needs to be simplified. Otherwise, there is little chance that an individual will know what redress they can have when things go wrong.

As is the case for other public service sectors, the Inquiry heard from a number of contributors that the devolved nature of healthcare service delivery raises ethical issues. The Inquiry heard evidence on the need for national ethical frameworks, and welcomed the publication on 19th February 2019 (following consultation) of a Code of Conduct for data-driven health and care technology. The Department for Health and Social Services intends this to set out "the behaviours we expect from those developing, deploying and using data-driven technologies, to ensure that all those in this chain abide by the ethical principles for data initiatives developed by the Nuffield Council on Bioethics: respect for persons, respect for human rights, participation, and accounting for decisions". In publishing the Code, the Department commits to engaging with the Centre for Data Ethics and Innovation on developing and monitoring the code to ensure it fits with the latest best practice.

Looking to future innovations, the Inquiry heard that greater use of data and machines would give rise to more complex ethical issues, for example whether decisions detrimental to the individual patient might be taken as a result of that patient having provided personal data or for reasons of value for money to the health service. Issues to be considered in future debates about data ethics include seeking to determine the boundaries of data capture and the implications for the nature of consent and privacy. Scientific innovation comes from connecting different datasets and argues for the broadest possible capture of data (environmental and social datasets as well as medical) even if the benefits are not yet obvious, to allow for exploitation as scientific knowledge develops. This could require different frameworks for consent.

[10] The NJR was set up by the Department of Health and Welsh Government in 2002 to collect information on all hip, knee, ankle, elbow and shoulder replacement operations, to monitor the performance of joint replacement implants and the effectiveness of different types of surgery.

The following are key findings from this strand of the Inquiry specific to Healthcare:

- Given the magnitude of the future prize from better use of data analytics and innovation, the benefits should not be jeopardized by relying on the implicit social settlement that NHS data may be used for general health purposes. The NHS needs to be more proactive and transparent with the public on issues of data, its use and sharing.
- The risk of an inconsistent experience on privacy depending on where you live argues for standardised ethics frameworks. The Code of Conduct for data-driven health and care technology is a good start, but needs to lead to a common approach in practice across NHS Trusts, especially in relation to data sharing that could result in data use for narrow commercial gain rather than common good.

Education

Universities collect data on students' activities and use analytical tools to target those with specific needs or who may be about to drop out of a course. A number of institutions provide this data to students so that they can monitor their own performance against that of their peer group. The Inquiry considered the following issues.

The Inquiry heard a number of examples of clear benefits in relation to helping students monitor their own performance and to provide triggers for intervention by tutors. However, the Inquiry was given clear examples of the limitations of data-driven decisions, particularly in making assessments that go beyond learner support, as algorithms may introduce errors through inherent bias (such as using data that is old or over which the student has no control): and consequently the importance of data as a tool to support, not replace, human judgments.

Inquiry members were sensitive to the fact that this is about young people at a formative stage in their life and career, and that bad decisions could have potentially devastating impacts on the individuals concerned, such as the thousands of international students whose visas were revoked due to a faulty algorithm in a voice matching algorithm.

As in other sectors, such as healthcare, there was a level of implicit consent to data collection, but trust should not be assumed as a contractual right, as this could fuel concerns that monitoring student attendance, library use, internet browsing and other activities is becoming sinister surveillance. Unsurprisingly, the Inquiry found that issues around third party data sharing were coming to the fore following the spotlight provided by the GDPR. It also heard, for example from Jisc, that there is a risk institutions might fail to use data for innovation purposes, particularly in Higher Education Institutions (HEIs) where data analytics programmes are motivated by administrative efficiency rather than to achieve educational objectives.

The following are key findings from this strand of the Inquiry specific to education:

- Data analytics must be employed by the institution for improved educational outcomes as well as for 'administrative' purposes if the full benefits are to be realised and an informed balance achieved between privacy and innovation.
- To maintain and develop trust in proper use of data there needs to be a transparent code of ethics that is consistent across education establishments, with students involved throughout its development.
- The importance of transparency in the factors underpinning decisions - when is it based on AI, and when on human interactions/judgements in face-to-face meetings between tutors and students where both sides can understand/agree the rationale.
- That practices across the HE sector are inconsistent and there should be better learning and consistency of approach. As in other public service sectors, the exploitation of data and technology to deliver common good while addressing issues of ethics and privacy calls for an independent Educational Data Ethics Advisory Board.

Policing

The use of data in policing attracted the widest range of views about privacy and bias versus effective service delivery for the common good. Police forces have for the past decade used algorithms but in relatively limited ways and largely for mapping - to identify areas of risk and prioritise resources. This has changed over the last couple of years, with a number of police forces starting to use predictive analytics in ways that more directly impact on individuals, such as to assess the likelihood of individuals reoffending. In April 2019, the Metropolitan Police announced the results of a study that used such data sets to find a link between current risks of knife crime and previous incidents[11]. With concern about some crime rates increasing, this makes it timely to consider issues of data ethics and trust.

Data is shared nationally and internationally to create databases of crimes and individuals, and to prevent organised crime and terrorism which do not respect geographical boundaries. The rapid increase in cybercrime requires police forces to understand data and technology, and to develop its use in order to try to be one step ahead of the criminal.

The risk of miscarriages of justice and the significant impact of ill-directed campaigns on communities and individuals from the use of AI, which - like stop and search - have all too often been connected with race, made this Inquiry theme the most controversial. There was wide divergence in views as to what might constitute beneficial technologies for policing, and whether police forces should develop predictive analytics and machine learning at all. The question was raised[12] as to whether national analytics solutions such as that described in a submission from the West Midlands Police would result in law enforcement moving into wider and deeper aspects of social and public policy, how desirable this would be, and the ethical issues it would raise.

The Inquiry heard that there are good examples of police forces setting up digital or data ethics panels, such as the Independent Digital Ethics Panel for Policing (encouraged by the National Police Chiefs' Council but membership is personal) and the London policing ethics panel (which for example has advised the Metropolitan Police on facial recognition trials). But the lack of overall government guidance on technology and ethics is a concern, particularly in this area given the operational independence of individual police forces and the "innovation" already undertaken by some forces.

As in other public service sectors, the Inquiry considered that the establishment of the Centre could be a force for good in helping provide an ethical framework providing a licence to operate that allows policing to develop beneficial data analytics for common good and to prevent harm.

The following are key findings from this strand of the Inquiry specific to policing:

- In this sensitive policy area, it is particularly important to do more on common ethical frameworks and codes of practice, and on fully engaging the public in the debate - or society would need to accept that common frameworks are not possible, with the attendant societal, cultural and political implications.
- The Centre should choose crime and justice as a priority sector in its forthcoming investigation of algorithmic bias.
- An official national ethics panel should be established to join up ethics debates across police forces and provide common guidance.
- There should be a national policy debate on the boundaries of law enforcement and its relationship to wider and deeper aspects of social and public policy.

[11] BBC News, Met detective 'predicts' fatal stabbing areas in London, 15th April 2019.
[12] Couchman H, Policing by Machine: Predictive policing and a threat to our rights, Liberty, January 2019 pg. 70.

Key Cross-Cutting Findings

The increasing reliance on the collection, storage, and use of data must be accompanied by governance improvements and the development of mechanisms that provide protection to individual rights and privacy, so as to improve public trust and retain support for technological change.

In 2018, researchers at the Alan Turing Institute found that "a legally binding 'right to explanation' for decisions made by algorithms was missing from the proposed GDPR, which could have harmful ramifications for people affected by such algorithmic processes"[13]. This was mirrored in the evidence submitted by the Oxford Data Institute to the House of Commons Science and Technology Inquiry into Algorithms and Decision Marking[14], which also noted a lack of any clear right or responsibility in this respect[15].

This is in contrast with other countries affected by GDPR who have introduced more direct regulation of the sector. In February 2018, the then French Minister for Digital, Mounir Mahjoubi, said that the government would not use any algorithms that did not have explicable decision making processes, a practical result of which was ensuring that the coding for the *Parcoursup* higher-education admissions application used open source software[16].

However, the UK has also been at the forefront of numerous innovations - ranging from the recognition of Artificial Intelligence and Data within the Industrial Strategy[17], to incentives such as NHSX to facilitate closer interactions between the health service, patient groups, and the life sciences sector[18]. This is vital to improving public engagement with new technologies and should provide a model for other government departments to follow.

Against that background the Inquiry identified the following cross-cutting findings:

[13] Alan Turing Institute, A right to explanation, July 2018.
[14] House of Commons Science and Technology Select Committee, Algorithms in decision-making, 15th May 2018, pg. 30.
[15] Oxford Internet Institute, Written evidence submitted by the Oxford Internet Institute (ALG0031), April 2017, pg. 5.
[16] Le Monde, Le ministère de l'enseignement supérieur dévoile l'algorithme principal de Parcoursup, 21st May 2018.
[17] HM Government, The Grand Challenges, 13th December 2018.
[18] HM Government, NHSX: new joint organisation for digital, data and technology, 19th February 2019.

Public Engagement and Trust

- Rules made with little or no public engagement have led to avoidable errors which could contribute to a public distrust in data use. The growing role of data in everyday life has in many cases occurred without consultation, and public agreement and a lack of engagement has compounded the damage caused to public trust through data breaches and misuse. The comparative ease of big data processing and the range of ways in which it can be used means that public understanding and consent is often partial and uninformed on the follow-on intentions for data collected. The Inquiry welcomes the focus the CDEI will be putting on public engagement issues.
- There are different assumptions across public services about levels of 'consent' whether informed or implicit, and about the extent to which the 'common good' test can and should be used to justify data collection, analysis and sharing.
- The public should be engaged through a wide variety of methods - including open consultations, town-hall meetings, industry outreach, and other ways of directly engaging with members of the public and relevant stakeholders.

Designing Ethical Technology and Data

- Ethical considerations must be tackled from the very start of developing or implementing transformational technologies to prevent a loss of public confidence and a withdrawal of the public "licence to operate".
- There are significant issues around intellectual property versus accountability and public trust: commercial intellectual property rights of technology firms makes algorithm-based decisions particularly opaque.
- The engagement of commercial organisations in the delivery of public services allows these organisations access to significant amounts of data. Third party use of data is a particular concern and citizens may feel differently about data-sharing with commercial bodies with the potential for loss of trust in the particular public service.

Consistent Experiences for Citizens

- There is a real risk that citizens and industry will have inconsistent policy and regulatory experiences across policy and geographical areas. Technology and data-driven investment could undermine broader national and devolved environmental and social policy objectives, particularly given the devolved nature of decisions on service delivery.
- The Centre will need to work very proactively across government - its role in developing a rules-based system must be clarified as this will support the join-up between it and other bodies. But the Centre can only do this effectively and easily if within each policy area there is a single point of focus at national level on data ethics. The new UK Artificial Intelligence Council announced by the government in the AI sector deal[19] provides another opportunity to join up the governance of data ethics: it could provide a link with ethics bodies in each government department and their arms-length bodies.
- The role of Parliament should be strengthened so as to bring in parliamentary input as part of improving transparency and scrutiny and a common ethical approach across the country.

[19] HM Government, Industrial Strategy: Artificial Intelligence Sector Deal, April 2018 pg. 20.

> **Another concern arises from the arrival of automated decision-making. ‘How are we going to operate these systems in a way where they can be challenged if the decisions they make are unfair?’ Grieve asked. He noted that the Windrush scandal illustrated the risk of bureaucratic mistakes. ‘If on top we are now going to factor in algorithms we are going to have to ask ourselves questions about what information are citizens going to be given, on data accuracy,’ he said. While automation has the potential to transform government for the better ’it is also possible to see how it has the capacity to act very badly indeed’.**

medConfidential submission to the Inquiry,
summarising a recent speech by
Dominic Grieve QC MP in the Law Society’s
rule of law lecture series, 20th September 2018.

Background –

Development of the Centre for Data Ethics and Innovation

The new Centre for Data Ethics and Innovation (CDEI, referred to as "the Centre") was announced in the 2017 Budget to develop the measures needed to strengthen and improve the way data and AI are used. In launching a consultation on the Centre on 20th November 2018, the Secretary of State for Digital, Culture, Media and Sport said[20]:

> **The Centre will make sure our society can [ ] maximise the benefits [these dramatic changes] bring. From helping us deal with the novel ethical issues raised by rapidly-developing technologies such as artificial intelligence (AI), agreeing best practice around data use to identifying potential new regulations, the Centre will set out the measures needed to build trust and enable innovation in data-driven technologies.**

The government did not envisage that the Centre should itself regulate the use of data and AI, but that as an advisory body it would set out best practice and advice on the effectiveness of and potential gaps in regulation.

This Inquiry started from the understanding that the establishment of the Centre for Data Ethics and Innovation is an important and positive step towards an ethical data framework. The Centre will play a pioneering role in shaping how data and AI are used, now and in the future, and ensure that data and AI-driven innovations deliver maximum benefits for society.

In its first 2-year strategy, published 20th March 2019, the Centre sets out the role it will play in supporting the aim of the UK becoming a global leader in responsible innovation in data-driven technology that benefits society as a whole:

- Seek to build a policy and governance environment that enables data-driven technology to improve people's lives
- Ensure the public's views inform the governance of data-driven technology
- Work to ensure governance of data-driven technology that can safely support rapid developments in the technologies and their applications
- Foster effective partnerships between civil society, government, academia and industry.

The government has already committed the Centre to developing data sharing frameworks as part of its initial work programme. The intention is that the Centre should play a key role in overseeing the development of such frameworks to ensure data can be shared in a safe, secure and equitable way to drive innovation.

The government has also committed the Centre to operating in a way that is transparent and open. It therefore proposes that its reports and recommendations are, by default, published at the point they are delivered to government - subject to any issues of national security. The government also proposes that, once firmly established, the Centre should consider making some or all of its board meetings open to the public. The Centre has committed to publishing a State of the Nation report in 2020.

The APPG on Data Analytics welcomes the establishment of the Centre but considers that more is needed in terms of governance and transparency across government. The Centre on its own will struggle to provide leadership across the whole of the wider public sector let alone the private sector. This Inquiry seeks to help in that by considering how ethical standards and frameworks need to be developed to enable innovation and provide a reliable, trusted jurisdiction for both individuals and companies, which in turn will provide the UK with a commercial advantage. It looks at four key areas of our lives: autonomous vehicles, healthcare, education, and policing.

[20] HM Government, Code of Practice: Automated Vehicle Trialling, February 2019, pg. 6.

Connected & Autonomous Vehicles

Technology and trust - benefits and challenges

The motor vehicle has been a fundamental part of society for over a century, transforming how individuals engage with their environment, and providing social and economic benefits through extending people's reach and independence. Wards Intelligence estimates that the global vehicle population stood at over 1.3 billion at the end of 2016, almost double the volume twenty years ago[21]. The soaring increase in take-up in China in recent years is likely to be followed in emerging economies such as in Africa and South Asia.

The automotive sector is facing a number of social, technological and environmental challenges. The environmental issues around the internal combustion engine and the loss of trust in relation to falsifying test results for diesel pollution levels need to be taken into account in considering how to tackle issues of ethics and trust in the technological shift offered by Connected and Autonomous Vehicles (CAVs), which for simplicity we have referred to as autonomous vehicles (AV).

Semi-automation is embedded in existing vehicles: a 2017 report by the Society of Motor Manufacturers and Traders (SMMT) identified that over half of the new cars sold in the country have at least one semi-autonomous driving feature and the vast majority have some form of connected technology[22]. As Professor Floridi has noted, autonomous vehicles stand as a typical example of how digital innovation in one sector is following the digital revolution, not leading it[23].

This familiarity of the technology and its benefits are reflected in some surveys of trust levels. A report by the SMMT in March 2017 noted that 56 percent of participants reacted positively to autonomous vehicles, with young people with disabilities being the group most excited. Three-quarters of these respondents said they trusted technology to some extent or to a great extent[24].

This reported level of trust should not be taken for granted. Perceptions will be impacted by incidents such as the death of a pedestrian caused by a driverless car undergoing trials in Tempe, Arizona[25]. Although prosecutors did not hold the company criminally liable[26], such incidents raise issues of accountability when things go wrong in relation to cars that 'drive themselves'. The Automated and Electric Vehicles Act of 2018 legally defines a vehicle as "driving itself" if it is operating in a mode in which it is not being controlled, and does not need to be monitored, by an individual[27]. This was expanded by a consultation led by the Law Commission, which led to the Department for Transport expanding the definition of a vehicle "driving itself" to include vehicles that can operate in an automated mode without direct human control. The definition also applies to those that do not require monitoring by an individual for at least part of a journey[28].

Other trust issues include ownership of the vast amounts of data that driverless and connected vehicles may collect on the movements and habits of individuals, and the so-called "trolley problem" in which, in what may be a very dramatic and unlikely crash scenario, the vehicle decides who lives and who dies.

[21] Petit S, World Vehicle Population Rose 4.6% in 2016, WardsAuto, 17th October 2017.
[22] SMMT, Connected and Autonomous Vehicles: Revolutionising Mobility in Society, March 2017, pg. 4.
[23] Floridi L, Soft Ethics, the governance of the digital and the General Data Protection Regulation, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Vol. 376, October 2018, pg. 2.
[24] Ibid, pg. 11.
[25] Guardian article, 19th March 2018.
[26] National Public Radio, 6th March 2019.
[27] HM Government, Automated and Electric Vehicles Act 2018, pg. 5.
[28] Law Commission, Automated Vehicles: A joint preliminary consultation paper, 8th November 2018, pg. i.

State and industry bodies are starting to invest heavily in AV technology, putting a premium on dealing with trust issues in parallel. In 2015, the government established the Centre for Connected and Autonomous Vehicles (CCAV), which has a remit to work across Whitehall to support the market for connected and automated vehicles. The Centre's mission statement sets out its roles and responsibilities:

> **The government believes that CAVs could change the way we travel, making road transport safer, smoother and more accessible to those with mobility issues. To this end, CCAV, a joint Department for Business, Energy & Industrial Strategy (BEIS) and Department for Transport (DfT) policy team, was established in 2015. By working closely with industry, academia and regulators, it aims to make the UK a premier development location for connected and automated vehicles. We are providing over £250 million in funding, matched by industry [across more than 70 collaborative projects], to position the UK at the forefront of CAV research, development and use. This will contribute to UK economic growth and help industry to develop safe, efficient systems to move goods and help people get around[29].**

AV technology also formed a key part of the Government's approach to building the modern Industrial Strategy. As part of the Mobility Grand Challenge, the government has set out a vision for the United Kingdom to become a world leader in autonomous vehicles and expects to see fully self-driving cars on UK roads by 2021. The stated benefits of automated transport include increased road safety, improved accessibility for the elderly and people with disabilities, and better use of urban space[30].

On the industry front, the Society of Motor Manufacturers and Traders in 2017 identified four challenges for the automotive industry[31]:

- **Car ownership:** the rise of car-sharing and private hire technology. Many automotive manufacturers are developing partnerships with major technology firms
- **Car user:** a transformation towards fully autonomous cars is likely to transform the relationship between consumers and vehicles
- **Data protection:** the collection and use of data by autonomous vehicles will require automotive manufacturers to accept high levels of scrutiny and trust in the collection, retention, use and protection of consumer data
- **Cyber security:** the increased interconnectivity of the automotive industry and manufactured products has given rise to greater demand for more robust security measures.

In sum, the investment in AV technology means that issues of public perception and trust will need to be tackled; and the Inquiry considered such needs to be a high priority before the technology is fully developed and deployed, with the public engaged by government and industry in debates around the ethics of AV technology now, rather than only in response to incidents causing loss of trust. Our report sets out proposals for public engagement to develop and maintain trust.

[29] HM Government, About Us, Centre for Connected and Autonomous Vehicles, March 2019.
[30] HM Government, Government kick-starts work on Future of Mobility Grand Challenge, 30th July 2018.
[31] SMMT, Connected and Autonomous Vehicles: Revolutionising Mobility in Society, March 2017, pgs. 18-19.

Policy and legal frameworks – adequate and coherent?

The UK government's initial focus has been on the policy and legal framework for trials of autonomous vehicles. In February 2019, the Department for Transport issued a consultation about updates to the Government's 2015 Code of Practice for AV trials[32]. The Code is not binding, but aims to provide guidance for those wanting to carry out "safe and responsible trials". A stated aim of the consultation is to improve engagement and transparency, and to improve public awareness and knowledge of trial activity[33]. Some contributors to this Inquiry felt the UK has a comparatively low bar for testing compared with other European jurisdictions, with two companies live-testing autonomous vehicles in London in 2019[34] and with a very low level of awareness among the public of where trials are taking place. Others contrasted the position in the UK and Europe with the fifty currently operating under licence, some without back-up drivers, in California[35].

Work has also begun on regulating the use of autonomous vehicles in the UK. In July 2018, the government passed the Automated and Electric Vehicles Act 2018, setting out a regulatory framework aimed at bringing automated vehicle insurance in line with "longstanding motor insurance practice"[36]. The Act ensures that British motorists are covered both when they're driving and when the driver has legitimately handed control to the vehicle.

The European Commission has been moving on new legislation on the subject of cooperative intelligent transport systems (C-ITS) and other uses for big data in the automotive sector, focussing for example on guaranteeing privacy and data protection. The EC considers that data coming from the vehicle and users is personal data[37]. Europe's stance on data from autonomous vehicles may be strengthened by its more recent moves[38] to tackle what the EU sees as anti-competitive and anti-privacy behaviours by big-tech firms that are inconsistent with privacy as a fundamental human right. This view of privacy may be particular to Europe: polls shows Europeans, and particularly Germans, to be more concerned about the use of their personal data by private companies than Americans are.

These cultural norms can be seen coming through the legal framework developed by the German government. In July 2016 the Federal Minister of Transport and Digital Affairs, Alexander Dobrindt, appointed a national ethics committee for automated and connected driving. A code of ethics was published the following year[39] and can be summarised as ensuring that the public is entitled to be informed about new technologies and their deployment wherever possible[40].

In the UK, a panel appointed in 2018 to examine digital competition chaired by former Chief Economist to President Obama, Professor Jason Furman, made recommendations in mid-March 2019 to open up digital markets, suggesting a regulator empowered to liberate data from firms to which such data provides "strategic market status"[41]. An EU panel with a similar remit is expected to make similar recommendations soon.

[32] HM Government, Government moves forward on advanced trials for self-driving vehicles, 6th February 2019.
[33] HM Government, Code of Practice: Automated Vehicle Trialling, February 2019, pg. 6.
[34] Oral Evidence, Autonomous Vehicles Roundtable, 4th December 2018.
[35] Shoot B, California Permits Waymo to Test Driverless Autonomous Cars on Its Streets, Fortune, 30th October 2018.
[36] HM Government, New powers to kick-start the rollout of electric chargepoints across the nation, 19th July 2018.
[37] European Commission, Public Support Measures for Connected and Automated Driving: Final Report, May 2017, pgs. 155-156.
[38] The Economist, Big Tech faces competition and privacy concerns in Brussels – and the sector may be the better for it. 23rd March 2019.
[39] Federal Ministry of Transport and Digital Infrastructure, Ethics Commission: Automated and Connected Driving, June 2017.
[40] Lütge C, The German Ethics Code for Automated and Connected Driving, Philosophy and Technology, September 2017.
[41] HM Government, Unlocking digital competition, Report of the Digital Competition Expert Panel, 13th March 2019, pg. 42.

The Inquiry heard that the introduction of autonomous vehicles could be highly disruptive in policy terms[42]. In their submission and literature review, Tom Cohen and Clémence Cavoli from the Centre for Transport Studies at University College London, highlighted five areas for government-led intervention[43] including planning and land-use, and regulation and policy. In the context of the United Kingdom, Cohen and Cavoli noted that some policy instruments are more applicable than others. For example, a prohibition on private AV ownership, whilst likely to be very effective in cutting numbers and congestion, is unlikely to be welcomed by private companies and members of the public[44].

This Inquiry identified a number of areas where there is a risk that broader government policy may be undermined by the development of AV technology, rather than its disruptive potential being put to use for the common as well as individual good.

A particular example relates to policies to reduce vehicle volumes in cities in order to improve health through lower air pollution and more active citizens. The Mayor of London's 2017 transport strategy set out a vision of 80 percent of all journeys in the Capital to be made by public transport, walking or cycling by 2041, representing a reduction in car trips by 3 million each day. The strategy also cites that not having to use a car must be the "affordable, safest and most convenient option for Londoners"[45]. In November 2018, Bristol set a goal of becoming carbon neutral by 2030, while Manchester said it would become 'carbon zero' by 2038. The future of autonomous vehicles in the UK should chime with the move in these cities towards increased use of public transport, buses and shared taxis.

Another potential policy gap relates to data capture from autonomous vehicles and whether existing information law is sufficient and adequate to take advantage of a world of interconnected, autonomous vehicles while at the same time protecting citizens' human rights.

The Centre for Connected and Autonomous Vehicles was set up to work across Whitehall, although this was prior to the creation of the Centre for Data Ethics and Innovation[46]. Cooperation, not competition, will be critical and - as we set out elsewhere in this report - the Centre needs to provide an overarching 'policy and regulation coherence' role. This is to manage the risk that policy decisions made by one Department could be overlooked by another, leading to regulatory failure or conflicting policy driving unintended consequences. Devolved government creates an additional risk of policy clash, calling for close engagement with devolved administrations and city mayors in particular.

[42] Oral Evidence, Autonomous Vehicles Roundtable, 4th December 2018.
[43] Cohen T and Cavoli C, Automated vehicles: exploring possible consequences of government (non)intervention for congestion and accessibility, Transport Reviews, Vol. 39 (1), 2019, pg. 138.
[44] Ibid pgs. 139-40.
[45] Greater London Authority, Mayor sets out ambitious plan to persuade Londoners to reduce car use, 21st June 2017.
[46] Oral Evidence, Autonomous Vehicles Roundtable, 4th December 2018.

What happens when things go wrong – who's accountable and what recourse is there for the citizen?

The Inquiry heard that the most extreme potential accountability issues may be over-dramatised. Ivana Bartoletti, Head of Privacy and Data Protection at Gemserv, expressed a view to that the so-called "trolley problem" (where the autonomous vehicle plays 'god') is highly unlikely to happen and can serve to alienate people from the wider benefits of AV as well as artificial intelligence in general[47]. However, there does need to be greater awareness, and testing with the public, of realistic safety issues around AV deployment to underpin future government decisions on the nature of regulatory approval that will be required before technologies reach the market. For example, on the extent to which fail-safe measures should be mandatory, and how to tackle the 'mixed economy' transition to full AV use, where safety will be at greater risk because humans are used to 'soft' interaction with one another - for instance reducing accident risk through eye-to-eye contact.

Whatever the levels of safety requirements, the issue of liability remains as accidents will happen. In relation to autonomous vehicles, this is likely to be around safety and security. In the context of accountability for deaths and injuries, Stilgoe recalls an incident in 2016 that resulted in the death of the 'driver' when the vehicle was on autopilot. He notes[48] that "despite a mass of information about what the car's machinery did in the minutes before the crash, the car's brain remained largely off-limits to investigators".

The Inquiry acknowledges there will be significant issues around intellectual property, against which accountability and liability issues need to be tested. Tackling this will involve challenging large market interests, ranging from established car manufacturers to service-providers and multinational tech firms. The EU's work is highly relevant here. Marina Jirotka and Alan Winfield made a case for an 'ethical black box'[49], modelled on aircraft black boxes, to enforce data sharing in robot systems so that people beyond just roboticists can learn from accidents[50]. In short - they are designed to provide explanations of their behaviour for accident investigation committees. In March 2019, the European Commission outlined plans to introduce mandatory safety devices, such as speed limiters, in all new vehicles by 2022. Likening the proposals to the introduction of seat belts, Commissioner Bieńkowska added that the proposals would also allow drivers and passengers to grow used to new technologies, stating "all this should enhance public trust and acceptance of automated cars, supporting the transition towards autonomous driving"[51].

Similar issues arise in relation to security liabilities. The government has begun to understand this. In 2017, the Department for Transport, in conjunction with Centre for the Protection of National Infrastructure, set out a list of eight principles for improving the cyber security of connected and autonomous vehicles[52], but further work is needed on accountability when things go wrong.

[47] Oral Evidence, Autonomous Vehicles Roundtable, 4th December 2018.
[48] Silgoe J, We Need New Rules for Self-Driving Cars, Issues in Science and Technology, Vol. 34 (3), March 2018.
[49] Winfield AFT and Jirotka M, The Case for an Ethical Black Box, Towards Autonomous Robotic Systems, TAROS 2017, Lecture Notes in Computer Science, Vol. 10454, 20th July 2017.
[50] Silgoe J, We Need New Rules for Self-Driving Cars, Issues in Science and Technology, Vol. 34 (3), March 2018.
[51] European Commission, Road safety: Commission welcomes agreement on new EU rules to help save lives, 26th March 2019.
[52] HM Government, The key principles of vehicle cyber security for connected and automated vehicles, 6th August 2017.

How can technology foster innovation?

Autonomous vehicles are linked with wider questions about the future of transport. Even the most optimistic assumptions about their future use can only be considered as part of wider questions. David Wong of SMMT highlighted wider policy goals such as improving air quality and road safety, as well as reducing congestion. The roundtable also noted how more efficient transport and use of roadspace can also form a key role in increasing economic productivity[53].

Improving mobility forms a major element of the Government's industrial strategy. A study by Ching-Yao Chan noted the impact that autonomous vehicles could play in addressing the challenges associated with an aging society in numerous ways[54]. In the UK, DVLA statistics show that in 2017 4.5 million of the 39 million people holding valid driving licences are aged over 70, with hundreds of thousands of motorists above the age of eighty[55].

Similar benefits could accrue to people with disabilities that impair their ability to travel. A lack of adequate independent transport can exclude people from employment, social life, education - as well as access to medical care[56]. By bringing together a range of supplementary connectivity and automation technologies, personal and public mobility can see a step change for elderly drivers and carers, as well as to society as a whole[57]. Policy makers must understand how autonomous vehicles can also be an enabler for better buses, trains and trams, as well as private vehicles[58].

Finally, the drive to open up access to data, with the consumer in the driving seat, offers opportunities for innovation. As an example of this, the Economist reported in a recent article on data and ethics[59] that enthusiasts of data sharing point to IBM, faced with antitrust action, divorcing its software and hardware businesses in 1969, thereby creating a new industry for software writers to explore.

[53] Oral Evidence, Autonomous Vehicles Roundtable, 4th December 2018.
[54] Chan C-Y, Advancements, prospects, and impacts of automated driving systems, International Journal of Transportation Science and Technology, Vol. 6, January 2017, pgs. 208–216.
[55] BBC News, Number of drivers aged over 90 tops 100,000 for first time, 26th July 2017.
[56] Bradshaw-Martin H and Easton C, Autonomous or 'driverless' cars and disability: a legal and ethical analysis, European Journal of Current Legal Issues, Vol. 20 (3), 2014.
[57] Yang J and Coughlin J F, In-Vehicle Technology for Self Driving Cars: Advantages and Challenges for Aging Drivers, International Journal of Automotive Technology, Vol. 15 (2), 2014 pg 338.
[58] Systra, Automated and autonomous public transport: Possibilities, challenges, technologies, 2018, pgs. 3-4.
[59] The Economist, Big tech faces competition and privacy concerns in Brussels, 23rd March 2019.

Healthcare

Technology and trust - benefits and challenges

As developments in care and prevention platforms develop, British healthcare systems are increasingly reliant on a range of data-dependent devices and services[60]. These have the collective ability to transform how patients and medical professionals interact with technology and to develop new forms of care, both within the NHS and in public health more generally. The Health Secretary, in his first speech in the role, suggested that the benefits of technology would be to expand access without further increasing pressure on the service[61]:

> **For too long, decisions on health and care have seemed to involve a trade-off - improving patient outcomes at the expense of placing ever more pressure on staff, while reducing the demands on staff has been seen to have an impact on patient care. Technology and data innovation offers an opportunity to move past this binary approach.**

In 2015 the Nuffield Council on Bioethics highlighted three key ways in which the responsible use of data can help to support scientific research and improve public wellbeing via improved healthcare, personal treatment and personal care[62]:

- Making health services more efficient through better informed decisions about how to allocate resources
- Improving health by building a stronger evidence base to predict, prevent and treat disease, developing new treatments and using data to personalise treatment and care
- Generating economic growth by driving innovation in the life sciences.

In a 2018 report, the industry body techUK sets out that the public is the “ultimate frontline of the NHS”[63] but that this opportunity has not yet been exploited through the development of large data sets and new approaches to outcomes. The report notes how the rise of smartphones and other forms of technology has given patients far greater control over their own care. This has been accompanied by a dramatic rise in the number of health-related apps, with 70 digital tools now featured in the NHS Apps Library[64], while a similar rise has been seen in the availability of wearable devices such as pedometers. These tools have given individuals more information than ever before about their lifestyle choices.

This technological shift has gone relatively unremarked by the general public. A report conducted by the market research firm, Ipsos Mori, for the Academy of Medical Sciences[65] showed that while there is optimism about new technology in healthcare (participants felt new technologies in general could increase efficiency, improve success rates of diagnoses, and save diagnostic time) there was low awareness of the types of data-driven technology discussed; how data is currently used; and how the NHS is organised, in particular its commercial partnerships.

[60] Ipsos Mori for the Academy of Medical Sciences, Future data-driven technologies and the implications for use of patient data: Dialogue with public, patients and healthcare professionals, November 2018, pg. 7.
[61] HM Government, Matt Hancock: my priorities for the health and social care system, 20th July 2018.
[62] Nuffield Council on Bioethics, The collection, linking and use of data in biomedical research and health care: Ethical Issues, November 2015, pg. 2.
[63] techUK, A Manifesto for Matt, October 2018, pg. 4.
[64] Ibid.
[65] Ipsos Mori for the Academy of Medical Sciences, Future data-driven technologies and the implications for use of patient data: Dialogue with public, patients and healthcare professionals, November 2018.

In contrast to other public institutions, public trust in the National Health Service has remained consistently high and public concerns have focussed on lack of staff, long waiting times, or insufficient government spending[66]. Turning to trust levels on the use of data by the NHS, a 2018 survey by the Open Data Institute indicated a high level of support for the use of personal data in the health sector, especially in contrast to other areas of public life. Key findings include[67]:

- 64 percent of consumers trust the NHS and healthcare organisations with personal data about them - ahead of friends and family (57 percent), banks (57 percent), local government (41 percent) and online retailers (22 percent)
- Nearly half of respondents (47 percent) would share medical data about themselves, if it helped develop new medicines and treatments, the most popular 'data trade off' in the survey.

A more recent study in 2019 by the British Heart Foundation and APPG on Heart and Circulatory Diseases also found high levels of support for the use of anonymised data - 86 percent of respondents were happy for their anonymised health data to be shared to better diagnose medical conditions, and 85 percent supported the use of AI in diagnostics and treatment. However, even higher numbers felt that the NHS should be informing the public about the use of AI in healthcare[68]. As issues of trust around technology rise up the agenda in society, these trust issues are likely also to become higher-profile.

The Inquiry considered that there are several aspects. There is the level of trust in the wider data ecosystem in the NHS, in other words its ability to protect data effectively against loss or theft. There is the question of what organisation will use the data, and the extent to which it is being used for the 'common good' or some other purpose. Ivana Bartoletti, Gemserv, advised that implied consent may be assumed for personal data being used to identify trends or traits within an NHS Trust, but this may be less likely to be the case if it is being used by private insurance firms to decide on premiums[69]. In 2017, the Department of Health said[70] that "Public confidence in data-sharing has been tested by several high-profile breaches of data security and confidentiality, while the NHS is still recovering from the controversy associated with the care.data programme".

[66] The King's Fund & Nuffield Trust, Public satisfaction with the NHS and social care in 2018, 7th March 2018.
[67] Open Data Institute, ODI survey reveals British consumer attitudes to sharing personal data, 12th February 2018.
[68] All Party Parliamentary Group on Heart and Circulatory Diseases, Putting patients at the heart of artificial intelligence, May 2019, pg. 19.
[69] Oral Evidence, Healthcare Roundtable, 8th January 2019.
[70] HM Government, Your Data: Better Security, Better Choice, Better Care, July 2017.

Policy and legal framework – adequate and coherent?

The long-term plan for NHS England, published in January 2019, suggested that digital technology will provide convenient ways for patients to access advice and care, with the interoperability of data across NHS structures being vital in achieving this transformation[71].

The Inquiry discussed that to achieve this objective the DHSC and NHS will need to address the devolved nature of NHS delivery and the level of autonomy in Trusts in setting their own policy and ethical frameworks. Andrew Davies of the Association of British Healthcare Industries highlighted the multifaceted legal framework and safeguards underpinning the use of data within the healthcare system[72]. Davies and others noted that the overall complexities at the regional and local levels result in most problems being associated with good governance and developing trusted relationships between different elements of the health sector. Each NHS Trust has its own processes, running the risk of different 'ethical contracts' with patients in different parts of the country. The Inquiry concludes that it is important for the DHSC, in conjunction with the Centre, and with the engagement of the public, to develop national ethical frameworks for use at the local and devolved level so as to standardise public experience and expectations.

The Inquiry heard that a particular issue which a standardised ethical framework should address is the levels of consent to be assumed depending on the purpose to which data would be put - a 'common good' test. Evidence given to the Inquiry stated that the concept of anonymisation was impossible to fully achieve in the context of large datasets within the NHS, in part due to the potential for data from different studies to be combined[73]. This was echoed by a recent report by The King's Fund[74], which notes the complexities and legal difficulties associated with the various opt-outs for the NHS and other medical providers under GDPR.

These issues test the position of the DHSC, as set out in 2017[75], that: "Safeguards governing the secondary use of patient data have been strengthened in recent years and will be bolstered by the implementation of a new national data opt-out alongside the introduction of the General Data Protection Regulation (GDPR) on 25 May 2018. These changes will not have any impact on depersonalised datasets, so most secondary analysis and research will be unaffected. However, analysis that relies on using confidential patient information - including some of the national patient surveys and specific efforts to evaluate NHS services and conduct research - may be affected".

In that document the Department acknowledged that NHS England and NHS Digital need to put in place a long-term plan to promote the benefits of data access and use, not least to avoid loss of trust leading to large numbers opting-out and thereby affecting the quality and validity of research. Our Inquiry felt that much more needed to be done on such engagements, in relation both to the sharing of data across the NHS and data sharing with third parties.

For example, in 2018 concerns were raised by the Health and Social Care Committee regarding the sharing of data between the NHS and the Home Office. A Memorandum of Understanding (MOU) had been agreed to allow the NHS to hand over patient data to the Home Office for immigration tracking purposes. However, the Select Committee said that it was not satisfied that the chief executive of NHS Digital had been sufficiently robust in upholding the interests of patients, understanding the ethical principles underpinning confidentiality, or in maintaining the necessary degree of independence from government. The MOU was suspended, and Home Office access to data was then restricted to the most serious of cases[76].

[71] NHS England, The NHS Long Term Plan, January 2019, pg. 25.
[72] Oral Evidence, Healthcare Roundtable, 8th January 2019.
[73] Bartoletti I, Oral Evidence, Healthcare Roundtable, 8th January 2019.
[74] The King's Fund, Using data in the NHS: the implications of the opt-out and GDPR, 25th May 2018.
[75] HM Government, Your Data: Better Security, Better Choice, Better Care, July 2017.
[76] Pharma Times, Gov't suspends controversial NHS data sharing deal, 10th May 2018.

What happens when things go wrong – who's accountable and what is the recourse for the citizen?

Experience to date shows that things will go wrong. Public trust in medical data capture has - as acknowledged by the Department for Health - been shaken by the care.data programme, established in 2013 with the aim of extracting data from GP surgeries into a central database. The means used by NHS England to communicate with the public and give them the ability to opt out was seriously flawed, which when exposed led to more than a million opts outs, negating the value of the programme. It was finally, after a number of other false starts, abandoned in 2016[77].

Another high profile case investigated by the Information Commissioner's Office (ICO) relates to a data-sharing partnership between the Royal Free Hospital NHS Trust in North London and the artificial intelligence company DeepMind. In April 2016, the Trust entered into an agreement with DeepMind to build an application called Streams, which used medical details to identify sufferers of acute kidney damage. However, a report by the New Scientist, also covered by national media outlets, exposed the fact that the agreement granted access to far more data than had been publicly announced. DeepMind was granted access to the details of all 1.6 million patients who were treated at the three hospitals run by the Trust. This included sensitive information regarding the details of individuals who were HIV-positive, suffering from drug overdoses, and having abortions[78]. Not all patients had even known that their data was being used to test the Streams software[79].

Key lessons from this failure are around data security and consent, and reinforce the need for proper public engagement in the development of data collection programmes, and gaining the right level of consent, if such consent is not subsequently to be withdrawn with major clinical and value for money implications. In the case of DeepMind, Dame Fiona Caldicott, the National Data Guardian at the Department of Health, concluded that she "did not believe that when the patient data was shared with Google DeepMind, implied consent for direct care was an appropriate legal basis"[80].

Following the ICO investigation, the Trust was asked by the Information Commissioner's Office (ICO) to[81]:

- Establish a proper legal basis under the Data Protection Act for the Google DeepMind project and for any future trials
- Set out how it will comply with its duty of confidence to patients in any future trial involving personal data.

Our Inquiry noted that these requirements were addressed to a particular Trust, not the NHS as a whole - how would lessons be learnt across Trusts? The Alan Turing Institute's Data Ethics Group, in their submission, highlighted the need for increased transparency, accountability and a process of ongoing assessment of data use by all NHS bodies.

How can technology foster innovation?

The Inquiry received a number of case studies showing the innovative solutions to be achieved through using big datasets[82]. For example, of retinal images to train and validate specific algorithms for a number of different purposes. The Moorfields AMD Clinical Dataset is a dataset containing over two million Optical Coherence Tomography - an imaging technique to develop highly detailed photographs. The project has led to a form of machine learning that has been able to effectively diagnose more than 50 sight threatening conditions with a 94 percent confidence interval, a level on par with that of a skilled ophthalmologist. Analyses of retinal scans is also leading to insights in long-term conditions. An ongoing project by the British Heart Foundation is currently exploring whether retinal blood vessels in the back of the eye can be used to identify long-term medical risks such as heart and circulatory disease, blood pressure and cholesterol[83].

[77] Guardian, NHS to scrap single database of patients' medical details, 6th July 2016.
[78] New Scientist, Revealed: Google AI has access to huge haul of NHS patient data, 29th April 2016.
[79] Information Commissioner's Office, Royal Free - Google DeepMind trial failed to comply with data protection law, 3rd July 2017.
[80] Sky News, Google received 1.6 million NHS patients' data on an 'inappropriate legal basis', 15th May 2017.
[81] Ibid.
[82] Abu-Bakir H and Fight for Sight, Submission to the Inquiry, November 2018.
[83] British Heart Foundation, Could our eyes reveal our future heart and circulatory disease risk?, 1st March 2016.

The Internet of Things offers a number of possibilities for the future of patient care. The increased connectivity of devices and other objects can be transformative, especially for self-treatment and end of life care.[84]

Finally, a study by IQVIA claims that rationalising the current plethora of mobile applications to a more curated model could lead to approximately £170 million in savings to the NHS's budget in terms of improved healthcare outcomes and efficiency savings[85]. Whilst comparatively small in contrast to the overall size of the NHS Budget, a narrow cost model does not take into account the wider social and economic value from giving individuals the tools to self-manage long-term conditions. Individuals experiencing conditions such as diabetes and asthma could take proactive action to have healthier lifestyles and improved mental and physical wellbeing.

The Inquiry heard that while algorithmic decision support in health is not a panacea, it's a technology that can significantly improve prevention and diagnosis of long term conditions. However, the examples of things going wrong suggests that innovation will be undermined if data is not shared in a transparent and informed manner, building public trust. In the DeepMind case the Information Commissioner, Elizabeth Denham, addressed the issue of innovation: "The Data Protection Act is not a barrier to innovation, but it does need to be considered wherever people's data is being used"[86].

Contributors felt there were reasons for optimism despite past false starts: there are indications that when properly engaged the public recognises the benefits of data used by the health service[87]. The key lesson remains the need to maintain and build on this trust through open consultation with the public about why the NHS uses data and how this can be best used to support the health and wellbeing of patients. This is particularly important in cases where the NHS proposes to share data with other public bodies and private companies.

The Inquiry heard that there are a number of different methods which can be used to improve data security and build public confidence in how their data is used. These include the establishment of 'data trusts' - a legal structure that provides independent third-part stewardship of data as defined by the Open Data Institute. Blockchain technology could provide a point-to-point consent solution or "trust layer" that establishes trust between the consenting and receiving parties[88].

The establishment of NHSX also has the potential to develop the links between Whitehall, the NHS, as well as the healthcare and pharmaceutical industries. The vision[89] towards open source code, creating a national policy and developing best practice for NHS technology, digital and data; facilitating better data-sharing and transparency; and reforming procurement processes is to be welcomed. However, it is vital that patients and medical groups are included in these discussions and developments. There is the risk that the body could become a sounding board for industry, limiting involvement by the citizen and patient in this vital area of public policy.

[84] Falzon D and Raviglione M, The Internet of Things to come: digital technologies and the End TB Strategy, BMJ Global Health, Vol 1 (38), 12th August 2016 .
[85] IQVIA, The Growing Value of Digital Health in the United Kingdom: Evidence and Impact on Human Health and the Healthcare System, November 2018.
[86] Information Commissioner's Office, Royal Free - Google DeepMind trial failed to comply with data protection law, 3rd July 2017.
[87] Open Data Institute, ODI survey reveals British consumer attitudes to sharing personal data, 12th February 2018.
[88] techUK, How Can Blockchain Help Solve the NHS Crisis?, 2nd March 2018.
[89] HM Government, NHSX: new joint organisation for digital, data and technology, 19th February 2019.

Education

Technology and trust - benefits and challenges

In 2017/18 there were 2.34 million students at UK Higher Education Institutions (HEIs), of whom just over 1 million were first-year students[90]. This was slightly higher than in the previous five years but below levels in 2008 to 2012 (the fee change took effect in 2012). Alongside this growth is a greater awareness of the importance of student experience for their educational and personal wellbeing, and an increase in the quantitative and qualitative data collected and collated by HEIs.

The data collected on students is multifaceted, and includes applications and admissions data, financial data, course data, attendance data, and student records data[91]. The holding of large volumes of data to guide everyday operations and strategic institutional decisions is not a recent phenomenon, but as in other sectors the scale of information and the purposes to which it is put have increased. The benefits to higher education of big data was described in a 2014 Horizon report by the New Media Consortium, for example that data collected on the online activity of students can be used effectively to identify the best learning resources, improve the student experience, and underpin success at university[92]. The Higher Education Commission, in its research publication From Bricks to Clicks, reinforced the benefits of data for learning analytics[93]: increasing retention; providing better feedback to students; and enhancing teaching and learning.

Inquiry participants also emphasised the benefits of adaptive-learning systems analysing student information to make course and career recommendations[94] and for predictive and pastoral reasons, including triggers for tutors of potential mental and physical health conditions. For example, the Nottingham Trent University's (NTU) learning analytics provides the University with early data to offer support to those students who may not be confident asking for help or are unaware that they may need it - tutors can see the normal patterns of engagement for their students and, in the most serious cases, will be sent an alert if their students have stopped engaging with their studies[95]. The Dashboard has been seen to help empower students - it provides another data source for students to help regulate their own engagement. Students can see, at a glance, their own engagement compared with their peers on their course.

The Inquiry also heard that HEIs are now looking outside their internal systems for data collection - from third party sources where the data is owned by others (e.g. tweets mentioning the HEI) to information on students commissioned by the institution but owned by third-party organisations[96]. During the Inquiry roundtable, Professor Eynon highlighted that data owned by third parties is of most concern in terms of maintaining trust in the gathering and application of data. She added that the role of commercial companies requires closer scrutiny than is currently being undertaken, and noted that student perceptions of how their data should be used may differ for this scenario in particular[97].

[90] House of Commons Library, Briefing paper on Higher Education Student Numbers, 8th February 2019.
[91] Higher Education Commission, From Bricks to Clicks: The Potential of Data and Analytics in Higher Education, September 2016, pgs. 16-17.
[92] Johnson L, Adams Becker S, Estrada V, Freeman A, NMC Horizon Report: 2014 Higher Education Edition, The New Media Consortium, 2014.
[93] Higher Education Commission, From Bricks to Clicks: The Potential of Data and Analytics in Higher Education, January 2016, pg. 14.
[94] Mara Richard of Civitas Education, Oral Evidence, Education Roundtable, 27th November 2018.
[95] Nottingham Trent University, Submission to the Data and Tech Ethics Inquiry, November 2018.
[96] Professor Rebecca Eynon, Submission to the Data and Tech Ethics Inquiry, November 2018.
[97] Professor Rebecca Eynon Oral Evidence, Education Roundtable, 27th November 2018.

There is a question mark over whether students implicitly accept that their university will collect data about their attendance at lectures and that their online attendance or visits to libraries will be recorded. Bodies such as the Higher Education Statistics Agency are able to use personal information under the proviso of informed consent - although largely for historic data[98]. Universities that have introduced specific student-facing tools, like NTU's Dashboard, advise that students report they trust the institution to use their data[99]. The University puts this down to defining strong ethical standards in policy documents, engaging student and staff users in the developmental stage, and introducing students to the policy during their induction. NTU stresses that learning analytics are only to be used to support learners and not as an assessment tool; they believe this reduces the need to have significant additional remediation mechanisms in place for cases where mistakes are caused by poor data or errors in the algorithm.

One particular data ethics and trust issue submitted to the Inquiry[100] relates to the fact that many commercially-available apps and software used in education are based on highly proprietorial systems and algorithms which, due to industry concerns around intellectual property and competition, are inscrutable to inspection. This makes it impossible for educators or students to understand how algorithms have been programmed and what error or bias may have been introduced. This issue is a broader one that the Inquiry encountered in other sectors.

Policy and legal framework – adequate and coherent?

The introduction of GDPR in May 2018 created a change in environment for the HEI sector. According to the Association for Learning Technology (ALT), the majority of institutions use contractual or other legitimate interests as the basis for using learner data, which does not require specific consent[101]. The ALT suggests that the full implementation of GDPR legislation, and best practice for informing learners about their rights, is still in progress. The Association, alongside other Inquiry participants, raised[102] the possibility of incorporating Slade and Prinsloo's proposed Analytics Ethics Framework into the wider regulatory framework for learning analytics. The Framework sets out six broad principles[103]:

1. Learning analytics as moral practice: the first principle is to appreciate that learning analytics is a moral undertaking and should not only focus on what is effective, but 'function primarily as a moral practice resulting in understanding rather than measuring'
2. Students as agents: institutions should 'engage students as collaborators and not as mere recipients of interventions and services'
3. Student identity and performance are temporal dynamic constructs: students' identities will change over the course of their studies, indeed education is often portrayed as an identity changing experience. Analytics and data need to take this into account
4. Student success is a complex and multidimensional phenomenon: student success and behaviour is a result of more than can be measured through data alone
5. Transparency: institutions should be transparent regarding what data is gathered and how it will be used
6. Higher education cannot afford not to use data: however it is part of an institution's responsibility to make moral and effective use of this data.

[98] Cormack A, A Data Protection Framework for Learning Analytics, Jisc, 30th June 2015, pgs. 11-12.
[99] Nottingham Trent University, Submission to the Data and Tech Ethics Inquiry, November 2018.
[100] Williamson B, Submission to All-Party Parliamentary Group on Data Analytics Inquiry into Data & Technology Ethics, Edinburgh Futures Institute, University of Edinburgh, (January 2019) pg. 4.
[101] Association for Learning Technology, Response from ALT's Members: Technology and Data Ethics Inquiry, January 2019, pg. 5.
[102] Association for Learning Technology, Response from ALT's Members: Technology and Data Ethics Inquiry, January 2019, pg. 3.
[103] Slade S and Prinsloo P., Learning analytics: ethical issues and dilemmas, American Behavioural Scientist, Vol. 57 (10) 2013, pgs. 12-14.

Participants at the roundtable noted the complexities associated with this approach to gathering data on students, especially from third party sources where consent for its use - or even collection - may be ambiguous. Although there are significant benefits to the use of data by institutions in order to plan for provision of services and support their students, a perceived lack of transparency about what is being monitored, how and by whom could prove particularly damaging. An ongoing study by Jisc[104] has found broad support for the three points highlighted by GDPR where institutions should:

- **Not ask** for consent for the use of non-sensitive data for analytics
- **Ask** for consent for use of special category data
- **Ask** for consent to take interventions directly with students on the basis of the analytics.

Jisc noted that six-in-seven of the "pathfinder institutions" in their study agreed with the framework highlighted above (the others adopted a "more conservative" approach).

In December 2018 the Education Secretary, Damian Hinds, called on universities to be more pro-active in using data to highlight educational challenges, and suggested that GDPR rulings could be relaxed to accommodate more intervention in this area[105].

What happens when things go wrong – who's accountable and what recourse for the citizen?

Universities have an established duty of care to young people, many of whom are living away from home for the first time. Whilst data can help with this role, it can also hurt the individual when mistakes are made, potentially irreparably. The Inquiry was given an example of a student who had been mortified when their disability was revealed to their lecturer, and the comment was made that although the scale (and therefore severity) of the error might be very low for the organisation committing it, for that individual it could be life-changing, opening up whether they even want to continue their course[106].

This reveals a contradiction in the current approach HEIs adopt with regard to the provision of data. They have a duty of care to students, whilst also having to abide by the rights individuals have to their own privacy. Policy makers must recognise the complex legal environment HEIs occupy in terms of how they use and collect data about those under their care. For example, the balance between dutiful and excessive monitoring: students have a level of implied consent, but this is not universal. One individual may begrudge having to swipe in for lectures, but swiping in may highlight someone who is not attending due to mental or physical troubles.

The Inquiry addressed the issue of bias in predictive analytics which could lead to deprioritisation of students assessed as more likely to drop out. Ben Williamson of University of Edinburgh in particular drew attention to the risk of mistakes resulting from predictive analytics:

> **Wrongly programmed or configured software and algorithms in ed-tech can have significant consequences for individuals when automated decisions are made based on faulty analyses of the data[107].**

[104] Jisc, Consent and the GDPR: what approaches are universities taking?, 30th June 2018.
[105] Daily Telegraph, Education Secretary backs system to flag university students' mental health problems to parents, 4th December 2018.
[106] Oral Evidence, Education Roundtable, 27th November 2018.
[107] Williamson B, Submission to All-Party Parliamentary Group on Data Analytics Inquiry into Data & Technology Ethics, Edinburgh Futures Institute, University of Edinburgh, (January 2019) pg. 8.

A high-profile example of the consequences for individuals is the widely reported action by the Home Office in relation to 34,000 international students and skilled migrant workers in the UK who were accused of cheating in an English language test. Following evidence that the government's decision in 2015 to revoke visas and threaten deportation may have been unsafe - the result of a faulty algorithm in a voice matching algorithm used in the English language tests that had incorrectly identified thousands of these students as 'cheats' - the NAO decided in 2019 to investigate the actions taken by the Home Office[107]. With multiple data sets being used by government, law enforcement and universities, and taking into account the highly international character of British HEIs, it is inevitable that further mistakes will be made unless interactions between education providers and other stakeholders are improved. This example also reveals important issues of accountability, with many of the affected students bringing their cases to court and senior lawmakers demanding an inquiry into the Home Office handling of the case.

Overall, however, the Inquiry heard that GDPR has given universities clearer responsibility for the use of data, and that students maintain a high-degree of autonomy over their own resources, with clearer avenues of accountability in the event of things going wrong.

How can technology foster innovation?

The Inquiry heard that the collection and analysis of data in higher education is often viewed as an administrative project[108]. This risks potential innovation being limited by overly prescriptive approaches undertaken purely to fulfil legal criteria. This would be contradictory and culturally damaging. As Professor Eynon noted[109]:

> **Questions of ethics are more likely to be reduced to questions of legal requirements, the focus will be on using the data to enhance efficiency of services, aspects of data work will be outsourced to commercial companies, and data projects become something that are 'done to' students and staff, typically to measure performance and compliance.**

HEIs need to properly consider what challenges big data can solve. Just as with other areas studied by the Inquiry, data should be used thoughtfully to improve higher education[110], not just because it is readily available. The Inquiry also noted that, whilst the nature of tertiary education has diversified markedly over recent years, there is still an assumption of a "one-size-fits-all" approach to how data is employed. Professor Eynon notes how the use of large scale data to measure drop-out rates is of greatest benefit for providers of distance learning, rather than full-time, campus universities where direct pastoral care would be of more direct benefit[111].

Learning analytics - especially predictive analytics - are still being developed at a rudimentary level and their long-term impact is something that will take time to fully understand. Data can never be expected to provide a full understanding of a student's academic abilities, their physical wellbeing, or their mental health. Evidence provided to the Inquiry by the University of Huddersfield referred to a scoping study carried out by the university on the use of machine learning to produce algorithms modelled to students' behaviours. This had identified a number of limitations, especially that weaker students made use of data to drive motivation whereas some stronger students found confronting their data emotionally challenging[112].

[108] https://www.nao.org.uk/work-in-progress/investigation-into-the-removal-of-international-students/ - dated Spring 2019.
[109] Oral Evidence, Education Roundtable, 27th November 2018.
[110] Eynon R, Submission to the Data and Tech Ethics Inquiry, November 2018.
[111] Biesta G, Good Education in an Age of Measurement: Ethics, Politics, Democracy, Routledge, 2015.
[112] Eynon R, Submission to the Data and Tech Ethics Inquiry, November 2018.
[113] Bennett L, Students' learning responses to receiving dashboard data, Society for Research into Higher Education, January 2018.

There are inconsistencies between HE institutions in the way data is used, with some universities reporting particular successes. This suggests that higher education providers would benefit from mechanisms to facilitate engagement with each other so that good practice can be supported and implemented more evenly across all institutions. The relationship between the university and the student is essentially a personal one, and data and technology in this sector particularly needs to use data as a tool to allow better judgements and develop better personal relationships with students, not as a substitute for the face-to-face.

Ben Williamson suggested that issues around consent can be resolved through the development of a new framework of “principles, values and purposes”[114]. These principles should be used to underpin data-informed education by educational institutions working in consultation with key stakeholders. Institutions should be encouraged and assisted to develop such frameworks, perhaps based on the sharing of best practice exemplars. The University of Edinburgh developed a “principles and purposes for learning analytics” statement, based on extensive stakeholder consultation, to ensure transparency, consent, ethics, privacy and access, and clarify data stewardship responsibilities such as retention and disposal of data[115]. A clear statement of intent such as this, readily accessible to students, is a vital aspect of building trust between them, their HEI, and the wider body politic.

As in the case of other sectors, it will be important that innovations address transparency and accountability so that it is clear to the student and the institution why particular judgements have been made; when a decision is based on AI rather than on human engagement, and if the former how the algorithm has been devised. This, as indicated elsewhere, has implications for the use of commercial applications and intellectual property issues versus transparency.

The Inquiry agrees with a suggestion made to it that an independent Educational Data Ethics Advisory Board should be set up with membership from professional practitioner groups, academic research centres, ed-tech industry bodies, student representatives and DfE. This is to ensure that policies and practices developed for data collection and use are driven by educational objectives (not just administrative neatness); take account of privacy and trust issues; involve all parties from the start (students and tutors); examine limitations of data exploitation as well as benefits; and consider issues for the UK’s skills base.

[114] Williamson B, Submission to All-Party Parliamentary Group on Data Analytics Inquiry into Data & Technology Ethics, Edinburgh Futures Institute, University of Edinburgh, (January 2019) pg. 8.
[115] University of Edinburgh, Learning Analytics Principles and Purposes, 22nd June, 2018.

Policing

Technology and trust - benefits and challenges

The use of data in policing was the most controversial of the four areas that the Inquiry considered in terms of privacy and bias versus effectiveness. There were strong views on both sides of the spectrum. Alongside evidence presented that greater use of analytics solutions could improve policing outcomes there were concerns[116] that technological solutions could result in law enforcement moving into wider and deeper aspects of social and public policy - and not necessarily overtly.

Historically, police forces in the UK have collected vast amounts of raw data on a day-to-day basis, but have often lacked the resources or technological ability to use it in an effective way[117]. Although predictive policing algorithms have been used for over a decade this has been broadly limited to mapping areas, to help identify locations at particular risk from crime and allocate resources accordingly[118]. Some field trials have suggested such tools may be around twice as successful in predicting the location of future crimes as traditional methods[119], but few police forces have incorporated them into their daily policing operations.

In the United States, the use of analytics has been more extensive, and consequently, more controversial. A 2016 investigation into the use of Correctional Offender Management Profiling by various county-level police forces found that black defendants were almost twice as likely to be deemed at risk of offending as white defendants[120]. Although disputed by the system's developer, a follow up report found that the programme was no more effective at making predictions about reoffending than an average member of the public[121].

In May 2017, Durham Constabulary became the first police force in the United Kingdom to use machine learning algorithms to assess the risk of individuals reoffending[122]. Their Harm Assessment Risk Tool uses a form of supervised machine learning to classify individuals by their likelihood of committing an offence over a two year period[123]. The system uses 34 variables, of which 29 relate to past criminal activity and the remainder being background information such as postcode, date of birth, and gender[124]. Liberty's study found that at least 14 police forces are currently using predictive policing programs, have previously used them, or are engaging in relevant research or field trials[125].

In the Royal United Services Institute's (RUSI) submission[126] to the Inquiry, Alexander Babuta noted four practical applications of big data technology to UK policing:

- Predictive crime mapping to identify areas where crime is most likely to occur
- Identifying risks associated with particular individuals, including people likely to reoffend, as well as those in need of safeguarding or becoming victims of crime
- Allowing police to better use data collected through visual surveillance, such as CCTV images and automatic number plate recognition
- Applying big data technology to open-source data, such as social media streams, to identify specific crime problems and better inform preventative policing strategies.

[116] Couchman H, Policing by Machine: Predictive policing and a threat to our rights, Liberty, January 2019, pg. 70.
[117] Babuta A, Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities, Royal United Services Institute, September 2017, pg. 9.
[118] Babuta A, Oswald M and Rinik C, Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges, Royal United Services Institute, September 2018, pg. 5.
[119] Ibid.
[120] Angwin J, Larson J, Mattu S and Kirchne L, Machine Bias, ProPublica, 23rd May 2016.
[121] Dressel J and Farid H, The accuracy, fairness, and limits of predicting recidivism, Science Advances Vol 4 (1) 17th January 2018.
[122] BBC News, Durham Police AI to help with custody decisions, 10th May 2018.
[123] Babuta A, Oswald M and Rinik C, Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges, Royal United Services Institute, September 2018, pg. 6.
[124] Oswald M, Grace J, Urwin S, and Barnes G C, Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, Information & Communications Technology Law, Vol 27 (2), 3rd April 2018, pg. 228.
[125] Couchman H, Policing by Machine: Predictive policing and a threat to our rights, Liberty, January 2019 pg. 45.
[126] Babuta A, Submission to the Inquiry, January 2019.

Boyd Mulvey, CEO of Chorus, a firm specialising in predictive analytics for police forces[127], advised the Inquiry of other potential benefits of technology and data to police forces, such as to draw together key information from crime scenes and develop courtroom reports[128].

Government policy on data technology in the criminal justice system appears more ambiguous than in other policy sectors. In his evidence, Alexander Babuta highlights the "noticeable lack" of government policy and guidance on how police forces can implement new technologies[129]. In both healthcare and education there is strong government support for the use of data and algorithms, but the Inquiry observed considerably greater reticence by policy makers to highlight their use by police forces[130]. The issues may not be confined to risk of discrimination but also to whether reductions in police budgets means such programmes are being used instead of, rather than alongside, human resources. In their Policing 4.0 report Deloitte found police leaders are "least confident about their ability to harness technology effectively and to co-ordinate effectively across policing organisations and geographies"[131].

Overall public trust in the police service remains high but the picture is complex with significant demographic and racial differences. The Office for National Statistics reported that in 2017/18, 78% of people aged 16 years and over in England and Wales said they had confidence in their local police - up slightly from 76% in 2013/14[132]. However, a lower percentage of people with mixed ethnicity reported having confidence in their local police compared with white people, and in each of the 5 years a lower percentage of black Caribbean people said they had confidence in their local police compared with white British people[133].

The use of predictive algorithms and machine learning has been controversial, with civil liberties organisations such as Liberty describing them as "opaque" and reliant on discriminatory profiling[134]. Such programmes have gained the most column inches and aroused the greatest attention (both positive and negative) from the public.

As in other sectors, trust in the ability of the service provider to use data effectively is impacted by trust on the basic issues of privacy and security. As reported by the Information Commissioner, in June 2018 Gloucester Police was fined £80,000 after sending a bulk email that identified victims of non-recent child abuse[135]. A failure to abide by GDPR will inevitably impact on trust levels and hence 'licence to operate' in relation to more sophisticated data use, such as using data sets to predict if people are more or less likely to commit crimes.

The Inquiry noted the challenges posed generally by devolved service delivery for a consistent data ethics approach and hence public trust, and this was also the case for policing. Alexander Babuta and others argued for a national framework to guide technological development for the police: to build trust in the police, forces need to adopt a common attitude at the national level to technology and ethics[136].

[127] Oral Evidence, Policing Roundtable, 15th January.
[128] Chorus, About Us, accessed 15th March 2019.
[129] Babuta A, Submission to the Inquiry, January 2019.
[130] Oral Evidence, Policing Roundtable, 15th January.
[131] Deloitte LLP, Policing 4.0: Deciding the future of policing in the UK, September 2018, pg. 21.
[132] Office for National Statistics, Confidence in the local police, 7th December 2018.
[133] Ibid.
[134] Couchman H, Policing by Machine: Predictive policing and a threat to our rights, Liberty, January 2019 pg. 3.
[135] Information Commissioner's Office, Gloucestershire Police fined for revealing identities of abuse victims in bulk email, 13th June 2018.
[136] Babuta A, Submission to the Inquiry, January 2019 pgs. 1-2.

Policy and legal framework - adequate and coherent?

As part of the Data Protection Act, the Government adopted the Police and Criminal Justice Data Protection Directive for the use of personal data for law enforcement. It requires public bodies to implement three separate forms of data processing procedures[137]:

- To deal with law enforcement data processed within the UK
- To deal with law enforcement data sent to or received from other member states
- GDPR to control the processing of all other personal data.

In March 2018 the Government set out that it would “update our data protection laws governing the processing of personal data for law enforcement purposes by the police, prosecutors and others”[138]. This would entail setting out the rights of law enforcement authorities and of individuals, with individuals’ rights being restricted “only where necessary and proportionate in order to: avoid obstructing an investigation or enquiry; avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security; and protect the rights and freedoms of others”.

In relation to data analytics, individuals’ rights include “rights in relation to automated decision-making (that is, decision making that has not involved human intervention)”. This right is defined by the Information Commissioners Office (ICO) as when “a potentially damaging decision is taken by solely automated means, i.e. without human intervention”[139]. The ICO guidance indicates this rarely occurs in the law enforcement context at the moment - but technological developments may change the position quite quickly if not managed, and legislators will need to address the legal framework for regulating their use and ensuring a balance between the rights of the individual against the need to protect the general public from harm.

In her submission to the Inquiry[140], Marion Oswald, Centre for Information Rights, noted that algorithms can be deployed at a number of stages by police forces - investigation, prosecution, post-conviction and for preventative purposes - and that this impacts the legal and political considerations behind their use. Their submission highlighted a programme being trialled by Norfolk Police which uses machine learning to predict how likely it is for a crime to be solved, as well as the extent to which resources should be committed to attempting to do so[141].

The Inquiry reflected that in relation to policing as a public service to improve citizens’ safety and security, the argument could be raised that authorities have an obligation to use machine learning and other data to ‘avoid harm’. But how this might translate into legal requirements is more complex and dependent on a demonstrably greater effectiveness of algorithms to achieve policing outcomes, balanced against the impact on human rights[142].

The Inquiry received an extensive submission by the Ethics Commission for the Police and Crime Commissioner for the West Midlands. This included an ethics advisory report prepared by the Alan Turing Institute for West Midlands Police (WMP). Both studies highlighted the growing expectations the public have on policing as a public service. In his review of the subject, Professor Floridi praised the establishment of an Ethics Committee by WMP to adopt a proactive approach to the use of data analytics. In particular, he cited that ethical frameworks go beyond legal compliance, into considering the social acceptability of the use of big and open data in the public realm[143].

[137] Chaucer, UK Policing and the GDPR, 4th January 2018.
[138] HM Government, Data Protection Bill Factsheet: Law enforcement processing, 5th March 2018.
[139] Information Commissioner’s Office, Right not to be subject to automated decision-making, retrieved 15th March 2019.
[140] Oswald M, Submission to the Inquiry, January 2019.
[141] Charette R, Norfolk Constabulary Using Controversial Algorithm to Help Decide If Burglary Investigation Warranted, IEEE Spectrum, 7th September 2018.
[142] Babuta A, Oswald M and Rinik C, Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges, Royal United Services Institute, September 2018, pg. 9.
[143] McNeil T, Report on the Stakeholder Engagement: Responses and Conclusions, West Midlands Police and Crime Commissioner, Autumn 2018, pg. 26-27.

The Inquiry considered a number of more general issues affecting policing at an international level. Whilst outside our domestic scope, they nevertheless highlight the increased interconnectivity between data sets, new technologies, and the relationship between the police and the general public. Cybercrime in particular was noted, with Professor Charles Raab and others raising the growing cost of transnational syndicates now using technologies such as blockchain to transfer funds and hide their activities. Misha Glenny's McMafia suggests that between 15 and 20 percent of GDP forms part of this so-called black or grey economy[144]. As new technologies arise, it is inevitable that policing - however local - will be affected by crimes being committed thousands of miles away. This highlights that building trust is not simply a question of the police using new technology effectively, it is also about ensuring that the public has confidence that such data is not being accessed by criminal elements.

What happens when things go wrong - who's accountable and what recourse for the citizen?

The consequences of things going wrong in policing can be on individuals (wrongly suspected of being criminals), communities (excessively targeted by the police) and the general public (resources poorly deployed). The stakes are high.

Evidence to the Inquiry was split on whether or not algorithms should form part of the policing process. Although predictive algorithms using machine learning are comparatively recent technology, algorithms have been used in policing for over a decade. In their 2019 report on predictive policing, Liberty highlighted four key areas of concern in the use of predictive algorithms by police forces in the United Kingdom[145]:

- Police algorithms entrenching pre-existing discrimination, where police officers are directed towards areas that already have disproportionate levels of police attention
- Predictive policing programs using discriminatory information in order to assess vulnerable people's chances of victimisation, such as being reported missing or being the victim of domestic violence or a sexual offence
- A lack of transparency and information amongst the public and serving police offices with regard to how predictive algorithms reach their conclusions
- The risk of automation bias where human decision-makers defer to computers and accept recommendations that may be incorrect or biased.

The risk of bias is seen to be particularly acute in relation to race. While models such as the Harm Assessment Risk Tool (HART) and the Correctional Offender Management Profiling for Alternative Sanctions tool do not include a variable for race, they do include the use of a postcode. In segregated areas, postcode can function as a proxy variable for race or community deprivation, thereby having an indirect and undue influence on the prediction[146]. With this in mind, the question also arises of how to take the decision or conclusions of an advisory algorithm into account. The HART model cannot draw upon information that legal professions, juries and judges would often take into account as mitigation, such as family circumstances[147]. As a result, there is the risk that "trial by machine" and automation bias may lead to the development of policing decisions that are simplistic and based on unsafe data, rather than drawing upon information that cannot be categorised, but would be invaluable to the criminal justice system.

[144] Glenny M, McMafia: A Journey Through the Global Criminal Underworld, Vintage, 2009, pg. 8.

[145] Couchman H, Policing by Machine: Predictive policing and a threat to our rights, Liberty, January 2019.

[146] Brennan T, Dieterich W, Ehret B, Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System, Criminal Justice and Behavior, Vol 36 (1), 20th October 2008, pgs. 21-40.

[147] Oswald M, Grace J, Urwin S, and Barnes G C, Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, Information & Communications Technology Law, Vol 27 (2), 3rd April 2018, pg. 232.

The Inquiry considered what Alexander Babuta and others claimed to be the most significant factor in the context of trust in policing - the problem of under-reporting. Many crimes go unreported, meaning that police data provides only an incomplete snapshot of the phenomenon under investigation[148]. Owing to the fact that arrest data is not necessarily representative of how crime is distributed the conclusions and assumptions made by the data may be inaccurate and fail to predict matters appropriately. If a particular neighbourhood has been disproportionately targeted by police action in the past, an algorithm may incorrectly assess that neighbourhood as being at increased risk of experiencing crime in the future. Acting on the predictions may then cause that neighbourhood to again be disproportionately targeted by police action, creating a feedback loop whereby the predicted outcome simply becomes a self-fulfilling prophecy.
Similarly, if a particular minority or social group has been disproportionately targeted by police action, the police may predict individual members of that group to be at increased risk of offending in the future. In reality, they may be no more likely to offend - just more likely to be arrested[149].

In terms of accountability when things go wrong, the Royal United Services Institute report explicitly noted the establishment of the Centre for Data Ethics and Innovation as a positive step, but remarked that the lack of a direct regulatory role by the Centre will impact its ability to have a meaningful impact on the practical application of predictive algorithms and machine learning[150]. The Inquiry heard that a single body - ideally outside the Home Office - should have oversight over how such programmes are deployed, and that an ombudsmen or regulator such as the Independent Office for Police Conduct would be well positioned to conduct this. This should be linked to a standardised set of terms and references for how such programmes are used and how ethics boards scrutinise and assess them.

How can technology foster innovation?

There were much more extreme views on future use of predictive analytics than in other policy areas, including whether to ban their use entirely. This is unsurprising given the potential for miscarriages of justice and other life-changing impacts on individuals, families and the wider community. However, it does make adopting meaningful recommendations more complex.

In his 2017 report, Alexander Babuta concluded that UK police forces are still a number of years away from being able to effectively implement any technology that is reliant on the use of big data[151]. He and others also noted that financial cuts in recent years have also hindered technological development and innovation by police forces, with many IT budgets being focused on supporting existing and increasingly outdated computer systems[152].

Professor Oswald also drew the Inquiry's attention to her summary of various case reviews over recent years which have recommended better use and sharing of information by and between agencies[153]. This was a common theme that emerged throughout: of encouraging better coordination between police forces. Whilst public opinion tends to support community policing and the image (however obsolete) of the "bobby on the beat", policy makers should be aware of the benefits to public safety and improving trust that can come from better data sharing. The solution for many problems regarding crime can often come from the better use of existing data, rather than feeling obliged to collate more.

[148] Babuta A, Submission to the Inquiry, January 2019.
[149] Ibid.
[150] Babuta A, Oswald M and Rinik C, Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges, Royal United Services Institute, September 2018, pg. 30.
[151] Babuta A, Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities, Royal United Services Institute, September 2017, pg. 9.
[152] Babuta A, Submission to the Inquiry, January 2019.
[153] Oswald M, Joining the Dots - Intelligence and Proportionality, Privacy & Data Protection, 2013.

In considering innovation in terms of predicting crimes from behaviour, there will be significant cultural differences that may preclude the sharing of tools internationally. Machine learning can often draw the wrong conclusions if deployed outside the country of origin. Vaak, a Japanese start-up that aims to prevent shoplifting by noting suspicious behaviour by individuals, may be completely irrelevant in a British context[154]. In some cultures, refusing to make eye contact is suspicious, in British cities it is part of the daily ritual of commuting.

Algorithms and data can approach these circumstances in different ways, however, this approach must not be to the detriment of individuals owing to biases in datasets. This puts a particular premium on understanding bias, and the Inquiry welcomes the Centre for Data Ethics and Innovation's study into algorithmic bias, and encourages it not to drop crime and justice from the areas to be considered in the study.

[154] Bloomberg, These Cameras Can Spot Shoplifters Even Before They Steal, 4th March 2019.

Contributors

Evidence Session One

Technology and Data Ethics Inquiry: Education
Upper Committee Room 18 – House of Commons
Tuesday 27th November 2018

Attendees	Position	Organisation
Mara Richard	Senior Director of International	Civitas Learning
Rose Luckin	Professor of Learner Centred Design	UCL Institute for Education
Louis Coiffait	Associate Editor	Wonkhe
Natalie Davis	Head of Government Relations	Centre for Data Ethics and Innovation
Christopher Conselice	Professor of Astrophysics	Nottingham University
Aaron Bowater	Outreach and Engagement Coordinator	Business and Local Government Data Research Centre
Rebecca Eynon	Senior Research Fellow and Associate Professor	Oxford Internet Institute
Sarah Sherman	Trustee	Association for Learning Technology
Jen Persson	Director	DefendDigitalMe
Neil McIvor	Chief Data Officer and Chief Statistician	Department for Education
Tony King	Director, Data in Government and Public Sector	Deloitte
Ben Williamson	Chancellor's Fellow	Centre for Research in Digital Education, University of Edinburgh
Jo Robotham	Head of Public Affairs and Media	Jisc
Iain Mansfield	Head of Public Sector	ACCA

Evidence Session Two

Technology and Data Ethics Inquiry: Autonomous Vehicles
Upper Committee Room 18 – House of Commons
Tuesday 4th December 2018

Attendees	Position	Organisation
Ivana Bartoletti	Head of Privacy and Data Protection	Gemserv
Jack Stilgoe	Senior Lecturer in Social Studies of Science	University College London
Amrita Ranchhod	Manager, Information Delivery, Analytics Information Management	Deloitte
Alan Winfield	Professor of Robot Ethics	University of the West of England
Mike Beevor	Senior Policy Manager	Transport for London
David Wong	Senior Technology and Innovation Manager	Society of Motor Manufacturers and Traders
Claire Gregory	Team Leader, Special Projects	Centre for Connected and Autonomous Vehicles
Niki Iliadis	Innovation and Policy Manager	Big Innovation Centre
Joseph Baddeley	Senior Policy Advisor	Centre for Data Ethics and Innovation
Alan Tua	Artificial Intelligence Lead	Deloitte

Contributors

Evidence Session Three

Technology and Data Ethics Inquiry: Healthcare
Meeting Room Q – Portcullis House
Tuesday 8th January, 2019

Attendees	Position	Organisation
Joe Johnson	Manager	Deloitte
Ming Tang	Director of Data, Analysis and Intelligence Services	NHS England
Tony King	Director	Deloitte
Charles Gutteridge	Chief Clinical Information Officer	Bart's Health NHS Trust
Ivana Bartoletti	Head of Privacy and Data Protection	Gemserv
Helen Kennedy	Chair of Digital Society	University of Sheffield
Edward Davis	Consultant Arthroplasty Surgeon	The Royal Orthopaedic Hospital NHS Foundation Trust
Andrew Davies	Digital Health Lead	Association of British HealthTech Industries
Chris Boulton	Associate Director, Research & Governance	Health Quality Improvement Partnership
Sam Smith	Coordinator	Medconfidential
Kerren McKinney	Director of Health Economics & Outcomes Research	Smith & Nephew
Andy Weymann	Chief Medical Officer and SVP for Clinical Research	Smith & Nephew

Evidence Session Four

Technology and Data Ethics Inquiry: Policing
Meeting Room Q – Portcullis House
Tuesday 15th January, 2019

Attendees	Position	Organisation
Ivana Bartoletti	Head of Privacy and Data Protection	Gemserv
Alistair Brown	Senior Manager Risk Analytics	Deloitte
Hannah Couchman	Policy and Campaigns Officer	Liberty
Charles Raab	Professorial Fellow	University of Edinburgh
Marion Oswald	Director	The Centre for Information Rights
Alexander Babuta	Research Fellow	
Boyd Mulvey	CEO	Chorus Intelligence
Edmund Koerber	Parliamentary Officer	Independent Office for Police Complaints
Stephen Canning	Councillor	Essex County Council
Zeynep Engin	Founder	Data for Policy
Katherine Mayes	Programme Manager	TechUK
Theo Knott	Policy Programmes Manager	BCA, The Chartered Institute for IT
Nicholas Dodd	Policy Manager	Centre for Data Ethics and Innovation

Acknowledgements

This report and its recommendations are the work of Policy Connect and the All-Party Parliamentary Group on Data Analytics, and the views and opinions expressed herein are the responsibility of Policy Connect.

Funding to support the work and expertise to inform our findings were provided by Deloitte and Jisc.

We also wish to thank all organisations that were consulted and provided submissions over the course of this project for their time and invaluable insights.

We recognise that these are complex and potentially controversial issues and expect that not all of those engaged will agree with every part of the report.

policy connect

Established in 1995, Policy Connect is a membership-based, not-for-profit cross party think tank working to inform, influence and improve UK public policy development and delivery. We lead and manage an extensive network of parliamentary groups, research commissions, forums and campaigns - bringing together academia, business and civil society with parliamentarians and government to develop new policy ideas through debate and research.

Policy Connect is also a London living wage employer and a Member of Social Enterprise UK.

The All-Party Parliamentary Group on Data Analytics is part of Policy Connect. This project was undertaken by Policy Connect's Industry, Technology & Innovation policy team.

Robert McLaren, Head of Industry, Technology & Innovation
Jack Tindale, Policy Manager, Industry, Technology & Innovation (Report Author)
Ben Carpenter Merritt, Policy Manager, Industry, Technology & Innovation
Geena Vabulas, Policy Manager, Industry, Technology & Innovation
Clive Gilbert, Policy Manager, Industry, Technology & Innovation

In addition, special thanks go to Omar Tellage, Oona Muirhead CBE, Louise Young and Jonathan Shaw.

Jisc

Jisc is a not-for-profit providing the UK's national research and education network, Janet, and technology solutions for its members – colleges, universities and research centres. It is funded by the UK higher and further education and research funding bodies and member institutions.

Jisc does three main things for its members:

- Operates and develops the super-fast and secure Janet Network and its built-in cyber security protection
- Helps save time and money by negotiating sector-wide deals with IT vendors and commercial publishers
- Provides trusted advice and practical assistance on digital technology

Jisc's vision is for the UK to be the most digitally advanced education and research nation in the world.

Deloitte.

We are led by a purpose: To make an impact that matters. Together we comprise tens of thousands of dedicated professionals throughout the world who collaborate to provide Audit & Assurance, Consulting, Financial Advisory, Risk Advisory, Tax and related services.

Our Risk Advisory practice advises organisations on how to effectively mitigate risk and make informed and intelligent risk decisions around business processes, technology and operations. We pride ourselves in taking an integrated approach, combining specialist insight and innovation across multiple disciplines including analytics, controls and resilience. Our business and industry knowledge helps you seize the opportunity to better manage your risks across a diverse range of topics be it from finance transformation to internal audit, or digital risk to credit portfolio management.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE' LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Documents Reviewed

Submission	Year	Title
ACCA	2019	Machine Learning: More Science than Fiction
Hassan Abu-Bakir	2018	Fight for Sight
The Alan Turning Institute	2018	The Alan Turing Institute Data Ethics Group
The Alan Turning Institute	2017	Ethics Advisory Report for West Midlands Police
Association for Learning Technology	2018	Response from ALT's Members: Technology and Data Ethics Inquiry
Alexander Babuta	2019	Submission to the Inquiry
Alexander Babuta	2019	Data Analytics and Predictive Policing: Legal, Ethical and Regulatory Challenges
Dr Liz Bennett	2018	Data and Technology Ethics Inquiry: Call for Evidence
Ching-Yao Chan	2017	Advancements, prospects, and impacts of automated driving
systems	2018	Home Office told thousands of foreign students to leave UK in error,
Tom Cohen and Clémence Cavoli	2019	Automated vehicles: exploring possible consequences of government (non)intervention for congestion and accessibility
Department for Digital, Culture, Media and Sport	2019	Introduction to the Centre for Data Ethics and Innovation
Department of Health and Social Care	2018	Annual Report of the Chief Medical Officer, 2018: Health 2040 - Better Health Within Reach
Zeynep Engin	2018	Digital Ethics: Data, Algorithms, Interactions
Rebecca Eynon	2015	The Quantified Self for Learning: Critical Questions for Education
Rebecca Eynon	2013	The rise of Big Data: what does it mean for education, technology, and media research?
Information Commissioner's Office	2018	Big data, artificial intelligence, machine learning and data protection
IQVIA Institute	2017	The Growing Value of Digital Health in the United Kingdom
Neil Lawrence and Stephen Bradley	2018	Big data and the NHS - we have the technology, but we need patient and professional engagement
Liberty	2018	Policing By Machine
Linklaters	2018	Audit of the acute kidney injury detection system known as Streams
medConfidential	2018	Submission to the APPG on Data Analytics
Nottingham Trent University	2019	Submission by Nottingham Trent University (NTU) to the Data & Technology Ethics Inquiry
Marion Oswald	2019	Technology and Data Ethics Inquiry: Call for Evidence
Personal Data Protection Commission: Government of Singapore	2019	A proposed model artificial intelligence governance framework
Brendon Shaw	2019	Technology and Data Ethics Inquiry
techUK	2018	Extracts from techUK's submission to DCMS' Consultation on the Centre for Data Ethics and Innovation
techUK	2018	A Manifesto for Matt: Shaping the vision for digital health and care
West Midlands Police and Crime Commissioner	2018	Report on the Stakeholder Engagement: Responses and Conclusions
Ben Williamson	2019	Submission to All-Party Parliamentary Group on Data Analytics Inquiry into Data & Technology Ethics

Author	Year	Title	Publication
Bayer R and Beauchamp DE	2007	Public health ethics: Theory, policy, and practice	Oxford University Press
Bennett L	2018	Students' learning responses to receiving dashboard data	Society for Research into Higher Education
Biesta G	2015	Good Education in an Age of Measurement: Ethics, Politics, Democracy	Routledge
Bradshaw-Martin H and Easton C	2014	Autonomous or 'driverless' cars and disability: a legal and ethical analysis	European Journal of Current Legal Issues
Brennan T, Dieterich W, Ehret B	2008	Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System	Criminal Justice and Behavior
British Heart Foundation	2016	Could our eyes reveal our future heart and circulatory disease risk?	British Heart Foundation
Brock, D. W.	1988	Paternalism and Autonomy	Ethics
Bundesregierung	2017	Ethics Commission: Automated and Connected Driving	Federal Ministry of Transport and Digital Infrastructure
Chaucer	2018	UK Policing and the GDPR	Chaucer
Deloitte LLP	2018	Policing 4.0: Deciding the future of policing in the UK	Deloitte LLP
Dressel J and Farid H	2018	The accuracy, fairness, and limits of predicting recidivism	Science Advances
Engin Z			2018
European Commission	2017	Public Support Measures for Connected and Automated Driving: Final Report	European Commission
European Commission	2018	Road safety: Commission welcomes agreement on new EU rules to help save lives	European Commission
Falzon D and Raviglione M	2016	The Internet of Things to come: digital technologies and the End TB Strategy	BMJ Global Health
Gouvernement de la République française	2018	Donner un sens à l'intelligence	AI for Humanity
artificielle: pour une Stratégie	2019	These Cameras Can Spot Shoplifters Even Before They Steal	Bloomberg
Floridi L	2014	Open Data, Data Protection, and Group Privacy	Philosophy & Technology
Floridi L	2018	Soft Ethics, the governance of the digital and the General Data Protection Regulation	Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences
Floridi L	2015	Toleration and the Design of Norms	Science and Engineering Ethics
Floridi L	2016	Tolerant Paternalism: Pro-ethical Design as a Resolution of the Dilemma of Toleration	Science and Engineering Ethics
Glenny M	2009	McMafia: A Journey Through the Global Criminal Underworld	Vintage
Hodson H	2019	Revealed: Google AI has access to huge haul of NHS patient data	New Scientist
Higher Education Commission	2016	From Bricks to Clicks: The Potential of Data and Analytics in Higher Education	Policy Connect
House of Commons	2019	Briefing paper on Higher Education Student Numbers	House of Commons Library
House of Commons	2018	Algorithms in decision-making	Science and Technology Select Committee
House of Commons	2017	Written evidence submitted by the Oxford Internet Institute (ALG0031)	Science and Technology Select Committee
House of Lords	2018	AI in the UK: ready, willing and able?	Select Committee on AI

Author	Year	Title	Publication
House of Commons	2018	Algorithms in decision-making	Science and Technology Select Committee
House of Commons	2017	Written evidence submitted by the Oxford Internet Institute (ALG0031)	Science and Technology Select Committee
House of Lords	2018	AI in the UK: ready, willing and able?	Select Committee on AI
House of Lords	2019	Regulating in a Digital World	Select Committee on Communications
King A and Crewe I	2013	The Blunders of Our Governments	Oneworld
Laslett P	1949	Patriarcha and Other Political Works	Blackwell
Law Commission	2018	Automated Vehicles: A joint preliminary consultation paper	Law Commission
Le Nevé S	2018	Le ministère de l'enseignement supérieur dévoile l'algorithme principal de Parcoursup	Le Monde
Locke J, Horton J and Mendus S	1991	A letter concerning toleration	Routledge
Lütge C	2017	The German Ethics Code for Automated and Connected Driving	Philosophy and Technology
McNeil T	2018	Report on the Stakeholder Engagement: Responses and Conclusions	West Midlands Police and Crime Commissioner
Mill J S	1859	On Liberty	Oxford University Press
NHS England	2019	The NHS Long Term Plan	Department of Health and Social Care
Open Data Institute	2018	ODI survey reveals British consumer attitudes to sharing personal data	ODI
Oswald M, Grace J, Urwin S, and Barnes G C	2018	Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality	Information & Communications Technology Law
Oswald M	2013	Joining the Dots - Intelligence and Proportionality	Privacy & Data Protection
Pinotsis D	2017	Towards a Legal Definition of Machine Intelligence: The Argument for Artificial Personhood in the Age of Deep Learning	International Conference on Artificial Intelligence & Law
Sclater N	2018	Consent and the GDPR: what approaches are universities taking?	Jisc
Schwab K	2016	The Fourth Industrial Revolution	Portfolio Penguin
Scoccia D	1990	Paternalism and respect for autonomy	Ethics
Silgoe J	2018	We Need New Rules for Self-Driving Cars	Issues in Science and Technology
Slade S and Prinsloo P		Learning analytics: ethical issues and dilemmas	American Behavioural Scientist
techUK	2018	A Manifesto for Matt	techUK
Thaler RH and Sunstein CR	2006	Nudge: Improving Decisions About Health, Wealth and Happiness	Penguin
University of Edinburgh	2018	Learning Analytics Principles and Purposes	University of Edinburgh
von Leyden W	1982	Hobbes and Locke: The Politics of Freedom and Obligation	Palgrave
Winfield AFT and Jirotka M	2018	Ethical Governance is essential to building Trust in Robotics and AI Systems	Philosophical Transactions A: Mathematical, Physical and Engineering Sciences
Winfield AFT and Jirotka M	2017	The Case for an Ethical Black Box, Towards Autonomous Robotic Systems, TAROS 2017	Lecture Notes in Computer Science

Data Collection

In November 2018 and January 2019, the APPGDA held four roundtable discussions in parliament, one on each of the four policy areas. These roundtables brought together a wide-range of industry figures, academics, campaigners and policy leaders to discuss and debate the challenges and opportunities such technologies provide.

The APPGDA also conducted an open call for evidence during this time - which called for submissions pertaining to the impact of data on new technologies, as well as for case studies in the four sectors of inquiry. The call for evidence was open from November 2018 and January 2019 and resulted in thirty individual submissions to the Inquiry.

Steering Committee

Darren Jones MP	Inquiry Co-Chair	House of Commons
Lee Rowley MP	Inquiry Co-Chair	House of Commons
Jonathan Shaw	Chief Executive	Policy Connect
Phil Richards	Chief Innovation Officer	Jisc
Marina Jirotka	Professor of Human Centred Computing	University of Oxford
Luciano Floridi	Professor of Philosophy and Ethics of Information	University of Oxford
Paul Garel-Jones	Partner, Risk Advisory	Deloitte
Narayanan Vaidyanathan	Head of Business Insights	ACCA

SUPPORTED BY

Jisc Deloitte.

CONTACT

Policy Connect
7-14 Great Dover Street
London SE1 4YR

@Policy_Connect
policy-connect
info@policyconnect.org.uk
☎ 0207 202 8585