HOUSE OF LORDS

Justice and Home Affairs Committee

1st Report of Session 2021–22

Technology rules? The advent of new technologies in the justice system

Ordered to be printed 21 March 2022 and published 30 March 2022

Published by the Authority of the House of Lords

HL Paper 180

Justice and Home Affairs Committee

The Justice and Home Affairs Committee was appointed by the House of Lords on 14 April 2021 to consider justice and home affairs, including the domestic criminal justice system, and international cooperation in respect of criminal justice, civil justice, migration and asylum.

Membership

The Members of the Justice and Home Affairs Committee are:

Lord Blunkett
Baroness Chakrabarti
Lord Dholakia
Baroness Hallett
Baroness Hamwee (Chair)
Lord Hunt of Wirral
Baroness Kennedy of The Shaws
Baroness Pidding
Baroness Primarolo
Lord Ricketts
Baroness Sanderson of Welton
Baroness Shackleton of Belgravia

Declaration of interests

See Appendix 1.

A full list of Members' interests can be found in the Register of Lords' Interests:
http://www.parliament.uk/hlregister

Publications

All publications of the Committee are available at:
http://www.parliament.uk/ 519/justice-and-home-affairs-committee/

Parliament Live

Live coverage of debates and public sessions of the Committee's meetings are available at:
http://www.parliamentlive.tv

Further information

Further information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is available at:
http://www.parliament.uk/business/lords

Committee staff

The staff who worked on this inquiry were Sam Kenny (Clerk), Achille Versaevel (Policy Analyst) and Amanda McGrath (Committee Operations Officer).

Contact details

General correspondence should be addressed to the Clerk of the Justice and Home Affairs Committee, Committee Office, House of Lords, London SW1A 0PW. Telephone 020 7219 6099. Email: HLJusticeHomeAffairs@parliament.uk

Twitter

You can follow the Committee on Twitter: @LordsJHACom

CONTENTS

Evidence is published online at https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law/publications/ and available for inspection at the Parliamentary Archives (020 7219 3074).

Q in footnotes refers to a question in oral evidence.

SUMMARY

In recent years, and without many of us realising it, Artificial Intelligence has begun to permeate every aspect of our personal and professional lives. We live in a world of big data; more and more decisions in society are being taken by machines using algorithms built from that data, be it in healthcare, education, business, or consumerism.

Our Committee has limited its investigation to only one area–how these advanced technologies are used in our justice system.

Algorithms are being used to improve crime detection, aid the security categorisation of prisoners, streamline entry clearance processes at our borders and generate new insights that feed into the entire criminal justice pipeline.

We began our work on the understanding that Artificial Intelligence (AI), used correctly, has the potential to improve people's lives through greater efficiency, improved productivity. and in finding solutions to often complex problems.

But while acknowledging the many benefits, we were taken aback by the proliferation of Artificial Intelligence tools potentially being used without proper oversight, particularly by police forces across the country. Facial recognition may be the best known of these new technologies but in reality there are many more already in use, with more being developed all the time.

When deployed within the justice system, AI technologies have serious implications for a person's human rights and civil liberties. At what point could someone be imprisoned on the basis of technology that cannot be explained?

Informed scrutiny is therefore essential to ensure that any new tools deployed in this sphere are safe, necessary, proportionate, and effective. This scrutiny is not happening.

Instead, we uncovered a landscape, a new Wild West, in which new technologies are developing at a pace that public awareness, government and legislation have not kept up with.

Public bodies and all 43 police forces are free to individually commission whatever tools they like or buy them from companies eager to get in on the burgeoning AI market.

And the market itself is worryingly opaque. We were told that public bodies often do not know much about the systems they are buying and will be implementing, due to the seller's insistence on commercial confidentiality–despite the fact that many of these systems will be harvesting, and relying on, data from the general public.

This is particularly concerning in light of evidence we heard of dubious selling practices and claims made by vendors as to their products' effectiveness which are often untested and unproven.

We learnt that there is no central register of AI technologies, making it virtually impossible to find out where and how they are being used, or for Parliament, the media, academia, and importantly, those subject to their use, to scrutinise and challenge them. Without transparency, there can not only be no scrutiny, but no

accountability for when things go wrong. We therefore call for the establishment of a mandatory register of algorithms used in relevant tools.

And we echo calls for the introduction of a duty of candour on the police to ensure full transparency over their use of AI given its potential impact on people's lives, particularly those in marginalised communities.

Thanks to its ability to identify patterns within data, AI is increasingly being used in 'predictive policing' (forecasting crime before it happens).

AI therefore offers a huge opportunity to better prevent crime but there is also a risk it could exacerbate discrimination. The Committee heard repeated concerns about the dangers of human bias contained in the original data being reflected, and further embedded, in decisions made by algorithms.

As one witness told us: "We are not building criminal risk assessment tools to identify insider trading or who is going to commit the next kind of corporate fraud … We are looking at high-volume data that is mostly about poor people."

While we found much enthusiasm about the potential of advanced technologies in applying the law, we did not detect a corresponding commitment to any thorough evaluation of their efficacy.

Proper trials methodology is fully embedded into medical science but there are no minimum scientific or ethical standards that an AI tool must meet before it can be used in the criminal justice sphere.

Most public bodies lack the expertise and resources to carry out evaluations, and procurement guidelines do not address their needs. As a result, we risk deploying technologies which could be unreliable, disproportionate, or simply unsuitable for the task in hand.

A national body should be established to set strict scientific, validity, and quality standards and to certify new technological solutions against those standards.

In relation to the police, individual forces must have the freedom to engage the solutions that will address the problems particular to their area, but no tool should be introduced without receiving "kitemark" certification first.

Throughout this report, we assign the national body a range of other duties. Key among them must be the establishment of a proper governance structure with the ability to carry out regular inspections.

We were told of more than 30 public bodies, initiatives, and programmes which play a role in the governance of new technologies in the application of the law.

Inevitably, their respective roles are unclear, functions overlap, and joint working is patchy. Government departments do not co-ordinate. No clear strategic plan can emerge out of such confusion, nor any mechanisms to control the use of new technologies. Certainly, it cannot be ascertained where ultimate responsibility lies.

The system needs urgent streamlining and reforms to governance should be supported by a strong legal framework. As it stands, users are in effect making it up as they go along.

Yet without sufficient safeguards, supervision, and caution, advanced technologies may have a chilling effect on a range of human rights, undermine the fairness of trials, weaken the rule of law, further exacerbate existing inequalities, and fail to produce the promised effectiveness and efficiency gains.

We acknowledge the good intentions of users, but good intentions are not enough. Legislation should be introduced to establish clear principles applicable to the use of new technologies, as the basis for detailed supporting regulation which should specify how these principles must be applied in practice.

Local specialist ethics committees should also be established and empowered. The law enforcement community has particular powers to withhold liberty and to interfere with human rights. They therefore have a corresponding responsibility to maximise the potential benefits of technology, while minimising the risks.

We are clear that the human should always be the ultimate decision maker–as a safeguard for when the algorithm gets things wrong, or when more information is required to make an appropriate decision. It is all too easy for an algorithmic suggestion to simply be confirmed with the click of a button.

Individuals should be appropriately trained in the limitations of the tools they are using. They need to know how to question the tool and challenge its outcome, and have the correct institutional support around them to do that.

There are no obligations for the consistent training of officials in the use of these systems. Even the police are not required to be trained to use AI technologies, including facial recognition.

We believe that there should be mandatory training for officers and officials on the use of the tools themselves as well as general training on the legislative context, the possibility of bias and the need for cautious interpretation of the outputs.

As the use of new technologies is becoming routine, these proposed reforms will ensure that we maximise their potential while minimising the associated risks.

They would reverse the status quo in which a culture of deference towards new technologies means the benefits are being minimised, and the risks maximised.

And they would consolidate the UK's position as a frontrunner in the global race for AI while respecting human rights and the rule of law.

Technology Rules? The advent of new technologies in the justice system

CHAPTER 1: INTRODUCTION

1. Government agencies and public bodies have long used technologies to support them in the course of their duties. Online databases, email, video-conferencing applications, and automated number-plate recognition are all examples of technologies that at one time were advanced but are now in common use. It is natural then, that as more—and more advanced—technologies develop, departments, agencies and police forces will look to use them to make their operations more efficient and more effective.

2. Our inquiry set out to examine the use of advanced technological tools, focusing on those which use algorithmic or machine learning technology in the application of the law. Within the application of the law, we included a broad view of the justice system, examining instances where advanced tools were used to discover, deter, rehabilitate, or punish people who breach the law in England and Wales, as well as border management. We did not, however, consider the use of modern technology in court processes such as the giving of evidence remotely; this is not 'new' technology and is the subject of study by others.[1]

Box 1: Definitions

Algorithm: a series of instructions for performing a calculation or solving a problem, especially with a computer. They form the basis for everything a computer can do and are therefore a fundamental aspect of all AI systems.[2]

Artificial Intelligence or AI: machines that perform tasks normally performed by human intelligence, especially when the machines learn from data how to do those tasks.[3] Tasks might include perceiving the environment, language translation, speech recognition, identifying patterns in large amounts of data, and making recommendations, predictions, or decisions. Some definitions of AI cover software packages that use data analysis, statistical and logic-based approaches, without necessarily needing to use machine learning.[4]

[1] See, for example, Constitution Committee, *COVID-19 and the Courts* (22nd Report, Session 2019–21, HL Paper 257).

[2] Artificial Intelligence Committee, *AI in the UK: ready, willing and able?* (Report of Session 2017–19, HL Paper 100), paras 9–12

[3] Office for Artificial Intelligence, Department for Digital, Culture, Media & Sport, and Department for Business, Energy & Industrial Strategy, *National AI Strategy* (22 September 2021): https://www.gov.uk/government/publications/national-ai-strategy [accessed 1 February 2022]

[4] For example, the definition in the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM(2021) 206 final.

Automated decision making (ADM): ADM is the process of making a decision by automated means without any human involvement. Decisions can be made based on factual data or inferred data. An example is a system counting correct answers on a multiple choice test sheet and then attributing a pass or fail mark based on the number of correct answers. It could also include an online decision to award a loan or provide a quote for the cost of a service.[5]

Data analysis: combining data from a variety of sources and applying organisational, statistical, mathematical or machine learning calculations to retrieve data, find a pattern, produce a conclusion or make a prediction.

Machine learning (ML): ML is a branch of AI that allows a system to learn and improve from examples without all its instructions being explicitly programmed. ML systems are provided with large volumes of different categories of data, and identify patterns that distinguish one category from another. Thus, they 'learn' to process future data, extrapolating its knowledge to unfamiliar situations. Applications of ML include virtual assistants (such as 'Alexa'), recommender systems, and facial recognition.[6]

Technological solution: a method by which data, digital software tools, AI and/or new technologies can be used (fully or partially) to provide a service, provide information, undertake a task, make a decision or change the way something is done.

The rapid deployment of new technologies

3. When we began our inquiry, we were aware of several technological solutions used in the application of the law. We had heard of 'predictive policing' which we understood as the use of historic data to predict where and when certain types of crime may be more likely to occur, and using those predictions to plan policing priorities and strategies. We were also aware of visa streaming algorithms—processing tools used by visa-issuing authorities to triage applications and decide which should be investigated. The use of facial recognition was of concern to us as well, especially in relation to privacy rights and risks of discrimination which have been widely reported.[7]

4. Written evidence from Dr Miri Zilka, Dr Adrian Weller and Detective Sergeant Laurence Cartwright laid out some categories of tools used in the justice system. While our scope is wider, most of the tools we heard of fit into these categories:

    (a) Data infrastructure: software and tools primarily used to record, store, organise, and search data.

[5] Information Commissioner's Office, 'What is automated individual decision-making and profiling?': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/ [accessed 6 February 2022]

[6] The Royal Society, *Machine learning: the power and promise of computers that learn by example* (April 2017): https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf [accessed 6 February 2022]

[7] 'UK's facial recognition technology 'breaches privacy rights'', *The Guardian* (23 June 2020): https://www.theguardian.com/technology/2020/jun/23/uks-facial-recognition-technology-breaches-privacy-rights [accessed 6 February 2022]. Also see Harvard University, The Graduate School of Arts and Sciences, 'Racial Discrimination in Facial Recognition Technology' (24 October 2020): https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ [accessed 6 February 2022].

(b) Data analysis: software and tools primarily used to analyse data to create insights.

(c) Risk prediction: software and tools primarily used for predicting future risk based on analysis of past data. This category can include predictions on an individual level (whether an individual poses a risk), or on a wider societal level (when and where a risk is higher).[8]

5. In the course of our inquiry, it became apparent that new technologies are used by a wide range of agencies to achieve a wide range of different purposes. We heard the most about tools used by the Home Office, the Ministry of Justice, HM Prisons and Probation Service, and individual police forces. They were being used for a variety of purposes, of which the following are examples:

- To provide efficiency. Eastern region police bodies have created a 'bot' to run procedural checks on vetting enquiries, passing key information to an officer for assessment and decision.[9]
- To provide new insights. Qlik Sense is a tool used by Avon and Somerset Police, which presents data in an interactive way. A police officer can see an increasing crime trend in their area, and find out quickly what crime types are driving that increase, along with specifics of the relevant offence.[10]
- To process large volumes of material. The Serious Fraud Office has used machine learning to pre-screen "several thousands of documents", thereby "saving up to two years and significant costs" compared to manual processing.[11]
- To screen documents. The Home Office uses an algorithm to help review applications for marriage licences. The tool can review applications and raise flags in the system to assist in launching investigations into a potential 'sham marriage'.[12]
- To provide risk assessments. Durham Constabulary has been using a Harm Assessment Risk Tool (HART), which uses data analytics and machine learning to provide a prediction of how likely an individual is to commit a violent or non-violent offence over the next two years.[13]
- To identify people. Automated facial recognition uses algorithmic technology to recognise people from pictures.
- To draw conclusions about people's emotions or deceptiveness. We were told, for example, about the use of polygraphs to monitor sex offenders on parole and manage their level of compliance with parole conditions.[14]

[8] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)

[9] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049)

[10] Written evidence from Avon and Somerset Police (NTL0052)

[11] Written evidence from the Serious Fraud Office (NTL0034)

[12] Written evidence from Public Law Project (NTL0046)

[13] Written evidence from Liberty (NTL0020)

[14] Written evidence from Dr Kyriakos N Kotsoglou (NTL0007)

6. These advanced technologies are developed and deployed to assist policing operations, prioritise tasks and support decision making. Artificial intelligence, algorithms and machine learning assist officers and officials in their jobs. They analyse data and provide an output, which a human decision maker then (in theory) uses to inform decisions. The aim behind the introduction of these technologies is to do the job (whatever it may be) better, faster, and more cheaply than was previously possible. Technologies can, for instance, take an image of a speeding vehicle and present officers with a number plate, removing the need for an officer to do so manually. They can call up information on an at-risk child, and they can provide a list of possible 'matches' for a person captured in a blurry CCTV frame who appears to be committing a crime.

Challenges and opportunities

7. We were drawn to this topic because we were concerned that the rapid increase in the use of new technologies, without a clear legal framework to ensure accountability and transparency, could cause injustice, and that the rule of law could be damaged.

8. Our evidence reinforced these concerns. One group of academics felt that some technologies will "mark a step change in police capabilities".[15] Another argued that "automated technology allows the police to go much further in monitoring individuals as they occupy public space than ordinary/human observation would."[16] These contributors felt that their use shifted "the balance of power between the citizen and the state and can undermine fundamental human rights and democratic norms."[17] Similar concerns of "potentially profound effects for society" were expressed by defenddigitalme.[18]

9. International examples were not reassuring. In the US, for instance, several law enforcement authorities purchased an AI-based predictive mapping service from a private company. An audit revealed several months later that the company had made false claims about the technology used and had had access to an excessive amount of personal data.[19] In the meantime, policing activities had been informed by the (paid for) "insights" shared by the company. In 2020, the City Council of Santa Cruz introduced a moratorium on predictive policing and facial recognition technology, arguing that these technologies "endanger civil rights and civil liberties" and "exacerbate racial injustice".[20] This decision was after almost a decade of use, by the Santa Cruz Police Department, of the PredPol software package—which Kent Police also used between 2013 and 2018.[21] Still in the US, Professor Joh told us about police forces being offered free trials of technological solutions, at

[15] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)

[16] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkiern and Professor Liz Campbell (NTL0021)

[17] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021)

[18] Written evidence from defenddigitalme (NTL0044)

[19] Letter from the Office of the Utah State Auditor John Dougall, to Attorney General the Hon Sean Reyes, *Re: Limited Review of Banjo* (26 March 2021): https://reporting.auditor.utah.gov/servlet/servlet.FileDownload?file=0151K0000042i9lQAA [accessed 7 January 2022]

[20] An Ordinance of the City Council of the City of Santa Cruz, 'Ordinance No 2020–17 Adding Chapter 9.85 "Surveillance Technology" to Article 9 "Peace, Safety and Morals" of the Santa Cruz Municipal Code' (23 June 2020): https://www.cityofsantacruz.com/home/showdocument?id=80906 [accessed 23 February 2022]

[21] *Ibid.*

the end of which it would become costly for the customer to opt out. She was clear that: "no free offer is ever truly free".[22]

10. Concerns must be addressed, because the rapid deployment of new technologies for the application of the law also entails clear benefits. A large number of contributors to our inquiry acknowledged the potential of these tools to increase efficiency and provide insight, assisting officers in the course of their duties. Avon and Somerset Constabulary thought their use of data analytics placed "better insights into the hands of those delivering the business to help empower and support more effective decision making."[23] The Rt Hon Kit Malthouse MP, the Minister for Crime and Policing at the Home Office and Ministry of Justice, told us that he was "very excited about the use of artificial intelligence and machine learning in policing."[24] We also acknowledge that, as many submissions pointed out, advanced tools can provide substantial assistance towards enacting the crucial duties of the police to protect and prevent harm. Our witnesses noted "enormous potential benefits such as increasing the capability of the police in ways that would not be possible without automation and new technologies".[25]

11. The potential of new technologies to provide new insight and enhance efficiency could increase the capabilities of departments, police forces, and public bodies more generally. If used appropriately, we were told that they do in fact have the potential to increase trust in the rule of law, as the use of analytical tools "bring a scientific basis to its application".[26] As the Information Commissioner's Office (the regulatory body for information rights) told us, "every technology can create benefits or risks depending on the context, governance and oversight measures, as well as its purpose."[27]

12. With this report, we set out to identify the necessary safeguards that will ensure we maximise the potential of new technologies while minimising associated risks.

The inquiry and the Committee's work

13. In May 2021, we decided to undertake an inquiry into the use of new technologies in the application of the law. On 22 July 2021, we launched a call for written evidence, which was shared with over 300 potentially interested parties. This can be found in Appendix 3. Over the course of several months, we reviewed 55 written submissions and spoke to 20 witnesses. We are grateful to our witnesses and contributors for their time and valuable input. A list of evidence, both written and oral, can be found in Appendix 2.

14. Our Specialist Adviser, Dr Marion Oswald, Associate Professor, Northumbria Law School, University of Northumbria, has been of immense assistance and we are extremely grateful to her for her expertise and advice. We are grateful also to members of the West Midlands Ethics Committee and to Deputy Police and Crime Commissioner Tom McNeil who facilitated our attendance at one of its meetings, and provided a private briefing on its work. Matthew Gill, Senior Fellow at the Institute for Government, facilitated a seminar for us to consider the institutional and regulatory frameworks which

[22] Q 45 (Professor Elizabeth Joh)
[23] Written evidence from Avon and Somerset Police (NTL0052)
[24] Q 99 (Kit Malthouse MP)
[25] Q 39 (Professor Elizabeth Joh)
[26] Written evidence from SAS UK&I (NTL0041)
[27] Written evidence from the Information Commissioner's Office (NTL0016)

may be put in place. The Parliamentary Office of Science and Technology and the House of Lords Library also provided valuable assistance.

Box 2: Previous work

This inquiry comes in the context of a variety of other national and international work.

- In 2017, the House of Lords Artificial Intelligence Committee published its report, *AI in the UK: ready, willing and able?*[28] This report concluded that putting ethics at the centre of the development and use of AI would enhance the UK's strong position to be a world leader in its development.
- In 2019, the Council of Europe Committee of Ministers appointed an Ad Hoc Committee on Artificial Intelligence to consider the feasibility and content of a potential legal framework on AI[29].
- In 2020, the Scottish Parliament Justice Sub-Committee on Policing published *Facial recognition: how policing in Scotland makes use of this technology.*[30]
- In 2021, the European Parliament Committee on Civil Liberties, Justice and Home Affairs published a report on "artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters".[31]
- In 2021, NATO adopted its first Artificial Intelligence Strategy, including principles of the responsible use of AI in Defence and announcing further work to set international AI standards.[32]
- In 2021, UNESCO adopted a Recommendation on the Ethics of Artificial Intelligence and is working towards establishing the first-ever global normative instrument on the ethics of AI.[33]

15. We decided to examine the use of these tools throughout the "criminal justice pipeline"[34] and in border management, identifying where change was needed, and identifying some principles for the safe and ethical use of such tools. We found, though, that this work had largely been done: academics and civil society alike have produced plenty of work which recommends worthy principles. What no one has quite done yet is to suggest how these principles should be brought together and put into practice.

16. In Chapter 2, we examine the need for a strategic approach and clear governance arrangements for the use of advanced technologies. We examine the legal framework and address a need for clear lines of accountability. In

[28] Artificial Intelligence Committee, *AI in the UK: ready, willing and able?* (Report of Session 2017–19, HL Paper 100)

[29] Council of Europe, CAHAI Ad Hoc Committee on Artificial Intelligence, 'Terms of Reference': https://www.coe.int/en/web/artificial-intelligence/cahai [accessed 6 February 2022]

[30] The Scottish Parliament, Justice Sub-Committee on Policing, *Facial Recognition: How Policing in Scotland Makes Use of This Technology* (1st Report, Session 5, SP Paper 678)

[31] Committee on Civil Liberties, Justice and Home Affairs, *Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (13 July 2021): https://www.europarl.europa.eu/doceo/document/A-9-2021–0232_EN.html [accessed 6 February 2022]

[32] North Atlantic Treaty Organisation, 'Summary of the NATO Artificial Intelligence Strategy' (22 October 2021): https://www.nato.int/cps/en/natohq/official_texts_187617.htm [accessed 6 February 2022]

[33] UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (2021): https://unesdoc.unesco.org/ark:/48223/pf0000380455 [accessed 6 February 2022]

[34] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)

Chapter 3, we look at transparency: its necessity and proposals to increase it. Chapter 4 deals with a crucial rule of engagement—the need always to have a human "in the loop"—and examines how this can be assured in practice. Chapter 5 concludes by focusing on scientific standards, procurement, and oversight.

17. The evidence we have received has been largely related to the use of advanced technologies by police forces, and this is inevitably reflected in the report that follows. The key issues we have identified, however, hold true for a much wider context: their application to all functions of the justice system and to border management. The conclusions and recommendations we have come to present a practicable way to develop the use of advanced technologies safely and ethically.

CHAPTER 2: LEGAL AND INSTITUTIONAL FRAMEWORKS

18. Those who most heavily advocated for the use of advanced technological tools in the application of the law tended to present them as tools which provided efficiencies and insight to assist in existing operations. We were told by the Home Office that "most data analytics used by police forces is currently used to enable organisational effectiveness and resource planning rather than directly to tackle crime."[35] The Minister described information collected by a machine learning tool as "a variety of pointers" and "a modern phenomenon of the police officer knowing who the bad lads were in the community."[36]

19. It was clear to us that in some cases, the use of advanced technological tools does not simply mark an extension of existing practices. Live Facial Recognition (LFR) technology, which is used operationally to tackle crime,[37] involves capturing and examining live footage of the public and was believed to "result in the further normalisation of surveillance across all society levels".[38] The use of polygraphs and other technologies believed to examine a subject's psychological or physiological responses are also more invasive than traditional practices.[39]

Rights-based concerns

20. Evidence was clear that the use of technologies in the application of the law spans a number of rights issues. A group of academics from the University of Essex listed these: "the right to freedom of expression; the right to freedom of assembly and association; and the right to freedom of thought, conscience and religion."[40] The Istanbul Bar Association wrote that their use can "directly affect freedom of expression; equality and non-discrimination; social and economic rights; fair trial; right to privacy; physical, psychological and moral integrity".[41]

21. It was also indicated that "public failures" could "lead to not just operational defects or inefficiencies, but miscarriages of justice",[42] and that where weaknesses were exposed, they "exacerbate the low level and negative trend in public trust for relevant technology".[43] Professor Nigel Harvey and Tobias Harvey referred to accountability for errors and misuse, saying that the use of algorithms "may leave people open to dangers for which no person can be identified as responsible".[44]

"A chilling effect"[45]

22. Various contributors told us that the use of some technologies, notably the use of live facial recognition, created fear or disquiet, and that this risked

[35] Written evidence from the Home Office (NTL0055)
[36] QQ 103–104 (Kit Malthouse MP)
[37] Royal Court of Justice, *R v The Chief Constable of South Wales Police*, [2020] EWCA Civ 1058. For more information, see Box 5.
[38] Written evidence from Privacy International (NTL0051)
[39] Written evidence from Dr Kyriakos N. Kotsoglou (NTL0007)
[40] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)
[41] Written evidence from the Istanbul Bar Association (NTL0028)
[42] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)
[43] Written evidence from Archie Drake and Perry Keller (NTL0011)
[44] Written evidence from Professor Nigel Harvey and Tobias Harvey (NTL0025)
[45] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021)

damaging the democratic process. Professor Charles Raab, Professorial Fellow of Politics and International Relations at the University of Edinburgh, was thinking about the future when he asked: "What would a change in the design or method of deployment of a camera, a sensor, or an algorithm mean in terms of exacerbating or ameliorating infringement of the freedom of assembly, privacy, and other rights enjoyed in a democratic society?"[46] Others referred to attendance at protests: "there will be some people who will not go to protests, for example, if they know that facial recognition is going to be used."[47] A group of academics even referred to a possible "chilling effect" on "public assemblies, freedom of expression, and the general use of public space by certain communities and demographics."[48]

Box 3: Automated Facial Recognition

1. Automated Facial Recognition technology consists of a technological solution matching biometric patterns to provide an assessment of whether two digital images depict the same person. When deployed in live settings, this technology is known as Live Facial Recognition (LFR).
2. LFR systems recently trialled (and now in use) by South Wales Police and the Metropolitan Police Service involve three main elements: 1) the real time capture of moving images via CCTV, for example of a location or event; 2) software that detects individual faces and turns them into numerical values; and 3) a database or 'watchlist' of existing facial images which have been turned into numerical values. When live footage has been captured, the system compares the facial values from the footage to the values from the watchlist.[49]
3. LFR systems do not guarantee a correct assessment of whether two images depict the same person. Most systems will generate a similarity score summarising the likelihood that two faces match. The similarity score will be generated by reference to whether the numerical biometric values have reached certain threshold levels. Fixing these levels inappropriately may create a risk of high false alarms or high false negatives.
4. Understanding how the similarity score and threshold values are set is therefore crucial to the assessment of the effectiveness, validity and accuracy of the system. There is also widespread concern that some LFR systems generate higher levels of false identifications for women and for people from black, Asian and other minority ethnic backgrounds.[50]

[46] Written evidence from Professor Charles Raab (NTL0014)

[47] Q 56 (Silkie Carlo), Written evidence from Liberty (NTL0020)

[48] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021)

[49] It appears that these trials have ended and that both forces are now using LFR operationally. See South Wales Police, 'Facial Recognition Technology': https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/ [accessed 6 February 2022] and The Metropolitan Police Service, *MPS LFR DEPLOYMENTS 2020:* https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf [accessed 6 February 2022].

[50] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021), Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035) and Big Brother Watch (NTL0037). For further information, see Chapter 5.

The right to a fair trial

23. We were concerned that, in some instances, the use of advanced tools at certain points of the criminal justice pipeline may impede an individual's right to a fair trial: whether by a lack of awareness that they were being used, unreliable evidence, or an inability to understand and therefore challenge proceedings. Dr Arianna Andreangeli thought that textual analysis tools could "adversely affect the ability of the investigated parties to have a reasonable opportunity to understand the charges made against them, to appreciate the assessment of the evidence made by the competition agencies and ultimately to build their own defence against these allegations."[51] Professor Elizabeth Joh, Professor of Law at the University of California, referred to the multiplicity of technologies that could be used in building a case, saying:

> "It is often very difficult for individual criminal defendants even to know what types of technologies might have been used in their particular case. Of course, that adds to the difficulty of raising challenges to a particular technology when you are not even sure what combination of licence plate reader data, facial recognition technology or predictive policing software might have led to the identification of you as a particular suspect."[52]

24. One contributor also told us that algorithmic technologies could be used without the court being made aware, and that in some cases, evidence may have been subject to "manipulation". David Spreadborough, a Forensic Analyst, gave the example that algorithmic error correction could be built into CCTV systems, and that "parts of a vehicle, or a person, could be constructed artificially",[53] without the court being aware.

25. Another contributor suggested that the judiciary may feel compelled to cede to algorithmic suggestions, and that this would render judges "the long arm of the algorithm".[54] Solid understanding of where advanced technologies may appear, how they work, their weaknesses, and how their validity will be determined is therefore a critical safeguard for the right to a fair trial.

26. **We see serious risks that an individual's right to a fair trial could be undermined by algorithmically manipulated evidence. We therefore favour precise documentation, evaluation by subject experts, and transparency where evidence may be subject to algorithmic manipulation.**

Equality

27. Technologies were seen to be reproducing inequities. Where the data fed to a machine learning programme was biased, the "resulting predictions are likely to present inaccurate or biased depictions of criminal activity", which Big Brother Watch thought likely to lead to "discriminatory policing interventions."[55] Liberty were similarly concerned that technologies which can be categorised as predictive policing "entrench pre-existing patterns of

[51] Supplementary written evidence from Dr Arianna Andreangeli (NTL0039). For further consideration of bias in facial recognition, see para 161.

[52] Q 44 (Professor Elizabeth Joh)

[53] Written evidence from David Spreadborough (NTL0015)

[54] Written evidence from Dr Kyriakos N. Kotsoglou (NTL0006)

[55] Written evidence from Big Brother Watch (NTL0037)

discrimination”,[56] and Professor Nigel Harvey and Tobias Harvey wrote that “learning algorithms based on historical data would preserve bias”.[57]

28. We do not have sufficient information to draw firm conclusions about the kind of crimes that are most heavily policed with algorithmic technology, but draw attention to a reflection from Professor Karen Yeung, Interdisciplinary Professorial Fellow in Law, Ethics and Informatics at the University of Birmingham, which suggests a concerning tendency:

> “We are not building criminal risk assessment tools to identify insider trading or who is going to commit the next kind of corporate fraud because we are not looking for those kinds of crimes, and we do not have high-volume data. This is really pernicious. We are looking at high-volume data that is mostly about poor people, and we are turning it into prediction tools about poor people. We are leaving whole swathes of society untouched by those tools.”[58]

29. In a similar vein, the logical consequence of ‘predictive policing’ tools, which indicate where crime is likely to occur, is that police officers patrol those areas. Liberty argued that areas identified in this way were likely to be “subject to over-policing (that is, a level of policing that is disproportionate to the level of crime that actually exist[s])”.[59] Due to increased police presence, it is likely that a higher proportion of the crimes that are committed in those areas will be detected than in those areas which are not over-policed. The data will reflect this increased detection rate as an increased crime rate, which will be fed into the tool and embed itself into the next set of predictions: a vicious circle.

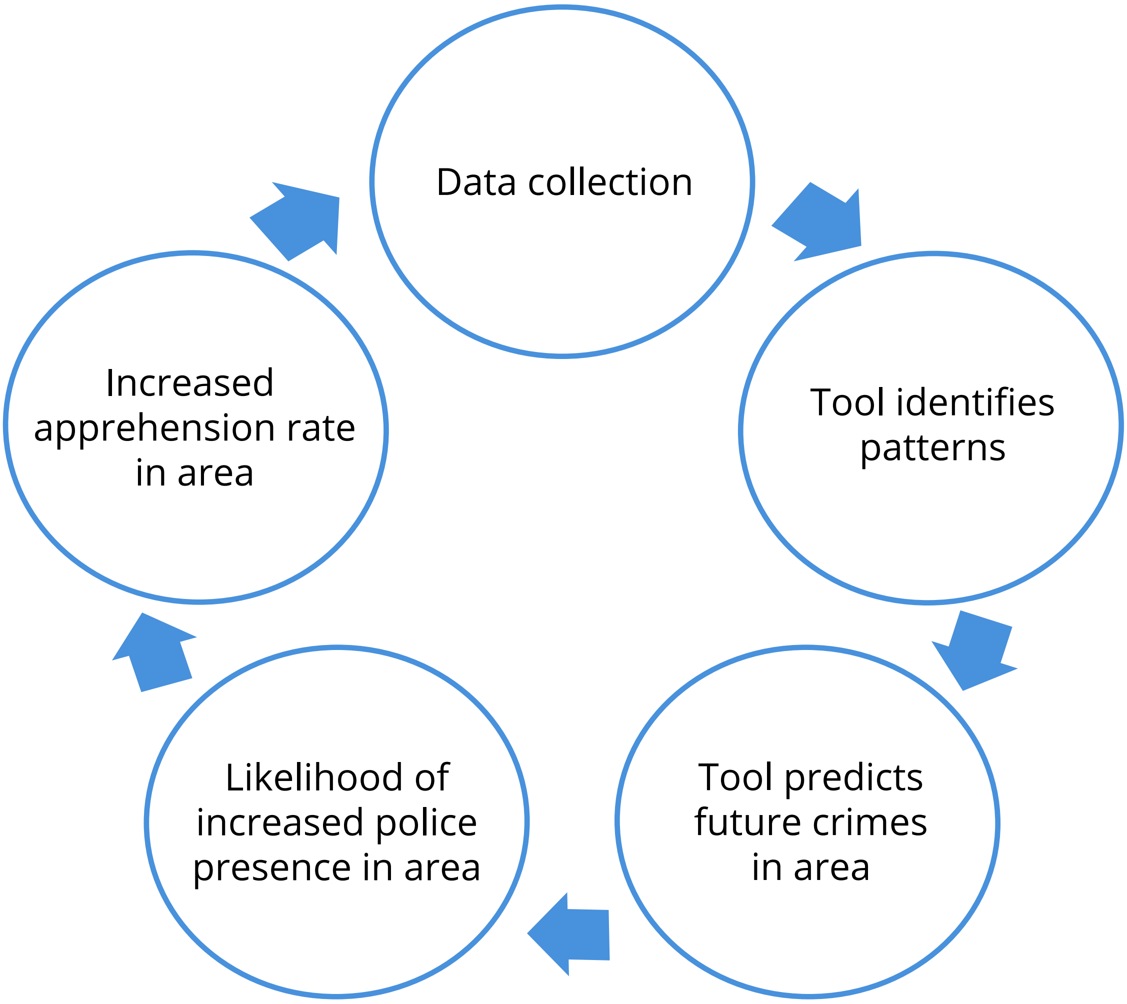
[56] Written evidence from Liberty (NTL0020)

[57] Written evidence from Professor Nigel Harvey and Tobias Harvey (NTL0025)

[58] Q 60 (Professor Karen Yeung)

[59] Written evidence from Liberty (NTL0020)

Figure 1: Predictive policing—a vicious circle?


Data collection
Tool identifies patterns
Tool predicts future crimes in area
Likelihood of increased police presence in area
Increased apprehension rate in area

30. **The use of advanced technologies in the application of the law poses a real and current risk to human rights and to the rule of law. Unless this is acknowledged and addressed, the potential benefits of using advanced technologies may be outweighed by the harm that will occur and the distrust it will create.**

Governance arrangements

31. Governance arrangements are essential as a basis for a clear, long-term strategy for the development of new technologies for use in the application of the law. Cohesion, consistency, and clarity are urgently needed in this area. The Minister for Crime and Policing, Kit Malthouse MP, described the "evolution":

> "Successive Governments have built on the structure of the past and no one has quite gone back to the beginning and said, 'Hold on a minute, if we'd known then what we know now, what structure would we have put in place?' Our job in all that is to set the frameworks legislatively and to adjust them through Parliament as required."[60]

32. We have noted over 30 public bodies, initiatives, and programmes playing a role in the governance of new technologies for the application of the law

[60] Q 99 (Kit Malthouse MP)

(see Box 4). They differ in size, remit, geographical scope, statutory status, longevity, and resourcing. Three of these bodies are worth mentioning specifically.

- The Office for AI is a joint BEIS-DCMS unit which is tasked with driving "responsible and innovative uptake of AI technologies"[61]. In September 2021, it published a National AI Strategy which "builds on the UK's strengths". It has three main aims: to invest and plan for the long term needs of the AI ecosystem; to support the transition to an AI-enabled economy, and to ensure that "the UK gets the national and international governance of AI technologies right."[62] To this end, a governance White Paper is expected to be published in 2022.

- The Centre for Data Ethics and Innovation (CDEI). The CDEI is a DCMS group tasked with "enabling the trustworthy use of data and AI". Its three key areas of work are "to pilot new forms of data stewardship and governance"; to increase assurance practices around AI; and, to assist public sector bodies looking to procure technologies—"facilitating the delivery of transformative data and AI projects in the public sector".[63]

- The AI Council is an independent advisory committee which "works to support the growth of AI in the UK" and aims to increase skills, "work on public perception", and "[explore] how to develop and deploy safe, fair, legal and ethical data sharing frameworks".[64]

[61] Office for Artificial Intelligence, 'About us': https://www.gov.uk/government/organisations/office-for-artificial-intelligence/about [accessed 6 February 2022]

[62] Department for Digital, Culture, Media and Sport, *National AI Strategy* (September 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402 [accessed 24 February 2022]

[63] Centre for Data Ethics and Innovation, 'About us': https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about [accessed 6 February 2022]

[64] HM Government, AI Council: https://www.gov.uk/government/groups/ai-council [accessed 6 February 2022]

Box 4: List of entities and programmes

- Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services
- The AI Council
- The Association of Police and Crime Commissioners (APCC), and its various working groups and initiatives, including the APCC Biometrics and Data Ethics Working Group
- The Biometrics and Forensics Ethics Group
- The Biometrics and Surveillance Camera Commissioner
- The Centre for Data Ethics and Innovation
- The College of Policing
- The Data Analytics Community of Practice
- The Equalities and Human Rights Commission
- The Forensic Science Regulator
- The Home Office Digital, Data and Technology function
- The Independent Office for Police Conduct
- The Information Commissioner's Office
- The National Crime Agency, and its TRACER programme
- The National Data Analytics Solution
- The National Digital and Data Ethics Guidance Group
- The National Digital Exploitation Centre
- The National Police Chiefs' Council, and its eleven co-ordination committees, each responsible for a specific aspect related to new technologies
- The National Police Ethics Group
- The National Policing Chief Scientific Adviser
- The Office for AI
- The Police Digital Service, its Data Office and Chief Data Officer
- The Police Rewired initiative
- The Police Science, Technology, Analysis and Research (STAR) fund
- The Police, Science, and Technology Investment Board
- The Royal Statistical Society
- The Science Advisory Council to the National Policing Chief Scientific Adviser
- The Senior Data Governance Panel within the Ministry of Justice
- The specialist and generalist ethics committees of some police forces
- The Tackling Organised Exploitation programme

33. It is very difficult to get a full picture. We are aware that some existing bodies were not mentioned in the evidence we received. Some of these omissions seem significant. The National Police Technology Council (NPTC), for instance, was not mentioned in evidence to us. Our knowledge on this entity is restricted to what little information is available online.

34. When we requested a "family tree" of the organisations involved in the governance of new technologies for the application of the law, Professor Paul Taylor, National Policing Chief Scientific Adviser, told us that "it may be more of a family bush".[65] Police representatives acknowledged that such arrangements may seem "unnecessarily complex"[66] ; and this is borne out by a DCMS consultation on data reform which refers to "crowded and confusing"[67] institutional arrangements. Kit Malthouse MP agreed that the institutional landscape "is quite a crowded field"[68] , which he attributed to our "model of decentralised policing".[69] Figure 2, shared with us by the Association of Police and Crime Commissioners, National Police Chiefs' Council, and the Police Digital Service , summarises the respective roles of some of these bodies.

[65] Q 98 (Professor Paul Taylor)

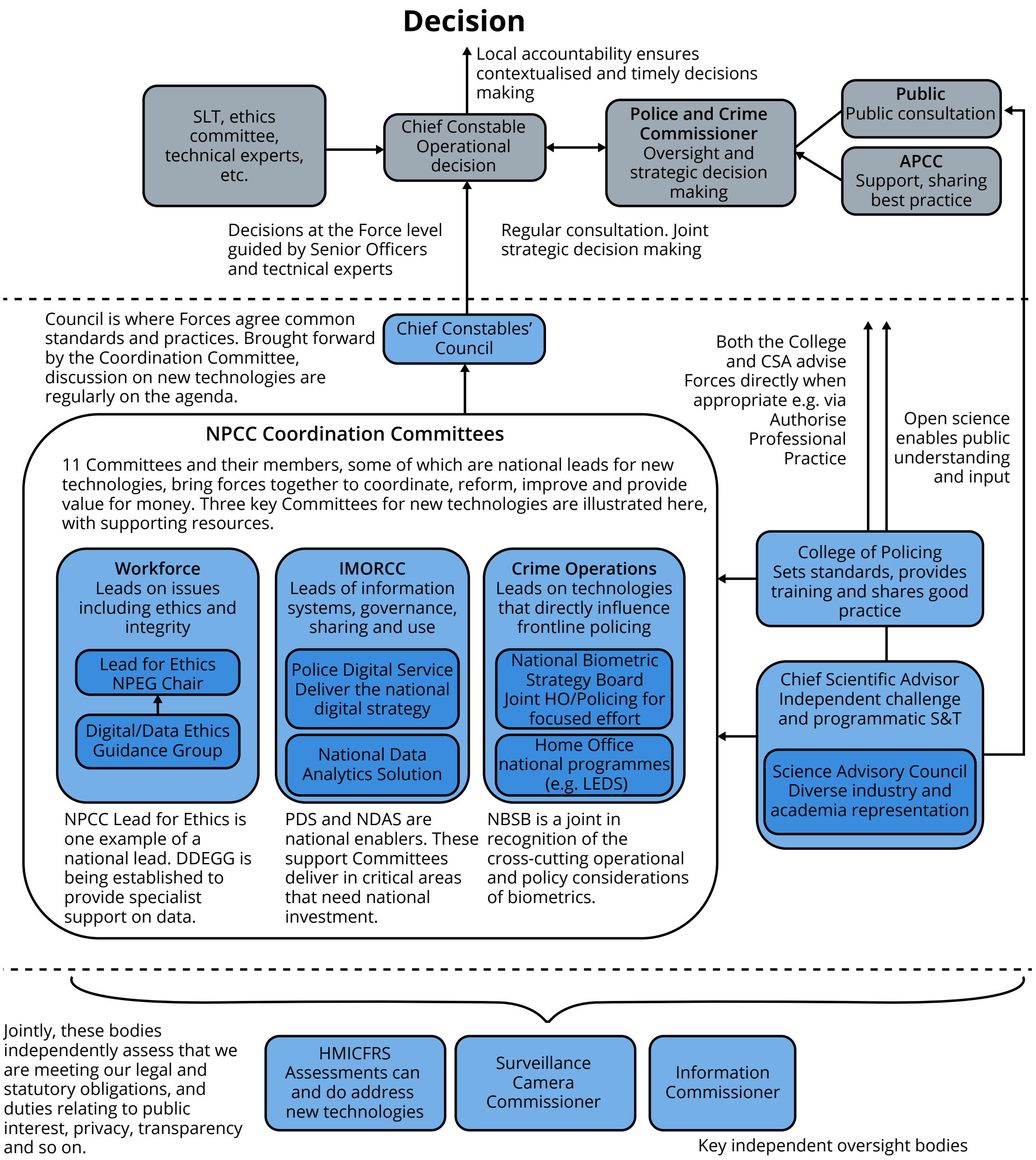
[66] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049)

[67] Department for Digital, Culture, Media & Sport, *Data: A new direction* (10 September 2021), para 409: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf [accessed 28 January 2022]

[68] Q 99 (Kit Malthouse MP)

[69] Q 108 (Kit Malthouse MP)

Figure 2: "Family tree" of relevant governance arrangements


Decision
SLT, ethics committee, technical experts, etc.
Chief Constable Operational decision
Police and Crime Commissioner
Oversight and strategic decision making
Public
Public consultation
APCC
Support, sharing best practice
Chief Constables' Council
NPCC Coordination Committees
Workforce
Leads on issues including ethics and integrity
Lead for Ethics NPEG Chair
Digital/Data Ethics Guidance Group
IMORCC
Leads of information systems, governance, sharing and use
Police Digital Service
Deliver the national digital strategy
National Data Analytics Solution
Crime Operations
Leads on technologies that directly influence frontline policing
National Biometric Strategy Board
Joint HO/Policing for focused effort
Home Office national programmes (e.g. LEDS)
College of Policing
Sets standards, provides training and shares good practice
Chief Scientific Advisor
Independent challenge and programmatic S&T
Science Advisory Council
Diverse industry and academia representation
HMICFRS
Assessments can and do address new technologies
Surveillance Camera Commissioner
Information Commissioner
Key independent oversight bodies

Local accountability ensures contextualised and timely decisions making

Decisions at the Force level guided by Senior Officers and tectnical experts

Regular consultation. Joint strategic decision making

Council is where Forces agree common standards and practices. Brought forward by the Coordination Committee, discussion on new technologies are regularly on the agenda.

Both the College and CSA advise Forces directly when appropriate e.g. via Authorise Professional Practice

Open science enables public understanding and input

11 Committees and their members, some of which are national leads for new technologies, bring forces together to coordinate, reform, improve and provide value for money. Three key Committees for new technologies are illustrated here, with supporting resources.

NPCC Lead for Ethics is one example of a national lead. DDEGG is being established to provide specialist support on data.

PDS and NDAS are national enablers. These support Committees deliver in critical areas that need national investment.

NBSB is a joint in recognition of the cross-cutting operational and policy considerations of biometrics.

Jointly, these bodies independently assess that we are meeting our legal and statutory obligations, and duties relating to public interest, privacy, transparency and so on.

Source: Supplementary written evidence from the Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0057)

35. In our months of inquiry, we heard a great deal about the complexity in governance arrangements. The number of entities and public bodies which have a role in the governance of these technologies indicates duplication and a lack of cohesion. Dr Christopher Lawless referred to a series of bodies that all play "key roles in oversight" but which "vary in their remit and the extent of their powers".[70] Robin Allen QC and Dee Masters believed that "there has been too much thinking in 'silos'".[71] There may also be confusion over responsibilities—Dr Lawless gave the example of facial recognition technology

[70] Written evidence from Dr Christopher Lawless (NTL0029)

[71] Written evidence from Robin Allen QC and Dee Masters (NTL0019)

to argue that there is a "potentially significant lacuna [in governance] where it is unclear who is statutorily responsible for regulation and oversight".[72]

36. Some of our witnesses saw value in the complexity of current institutional arrangements. Police representatives told us the "federated structure … enables local flexibility and accountability while providing redundancy and important checks-and-balances, which support rather than impede local decision making."[73] Dr Christophe Prince, Director for Data and Identity at the Home Office, also noted that current institutional arrangements ensured a degree of resilience because each body can add "their own expertise", "be that commercial or scientific".[74]

37. There are several initiatives to simplify and harmonise the existing institutional landscape:

- In January 2020, the National Police Chiefs' Council (NPCC) and the Association of Police and Crime Commissioners (APCC) launched the Policing Digital Strategy 2020–2030.[75] Its ambition is to achieve "the right infrastructure and the right governance" within a decade.[76] This involves the development of national capabilities to "propagate best practice and remove duplication".[77] Current national capabilities notably include the Police Digital Service (PDS), the National Digital Exploitation Centre (NDEC), and the National Data Analytics Solution (NDAS).[78]

- In March 2021, the Government merged the posts of the Biometrics Commissioner and the Surveillance Camera Commissioner into a single Biometrics and Surveillance Camera Commissioner to reflect the "growing partnership between those two technologies".[79]

- In May 2021, the first National Policing Chief Scientific Adviser was appointed. The postholder, Professor Paul Taylor, described his role as providing "oversight and advice to all those moving parts in the hope that they are moving in the same direction in a way that benefits and supports Chief Constables and Police and Crime Commissioners in their ultimate decision-making."[80]

[72] Written evidence from Dr Christopher Lawless (NTL0029)

[73] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049)

[74] Q 108 (Dr Christophe Prince)

[75] National Police Chief's Council, Association of Police and Crime Commissioners, *National Policing Digital Strategy Digital, Data and Technology Strategy 2020–2030*: https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020–2030.pdf [accessed 26 January 2022]

[76] Q 108 (Kit Malthouse MP)

[77] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049)

[78] The National Data Analytics Solution is a scalable and flexible analytics capability for law enforcement which aims to develop capacity to use data analytics to deliver insights to partners. It is a Home Office sponsored project being implemented by West Midlands Police. For more information, see West Midlands Police, 'National Data Analytics Solution': https://west-midlands.police.uk/about-us/privacy-notice/national-data-analytics-solution [accessed 17 March 2022].

[79] Q 99 (Kit Malthouse MP), see also Home Office, *New Biometrics and Surveillance Camera Commissioner appointed* (15 March 2021): https://www.gov.uk/government/news/new-biometrics-and-surveillance-camera-commissioner-appointed [accessed 28 January 2022]

[80] Q 84 (Professor Paul Taylor)

- In September 2021, the Government published its *National Artificial Intelligence Strategy*. Presented as a "ten-year plan to make Britain a global AI superpower", the AI Strategy aims to develop better governance to "encourage innovation, investment, and protect the public and our fundamental values." Arising from the strategy, the Government is expected to publish a White Paper on AI Governance in 2022.[81]

- In September 2021, the Department for Digital, Culture, Media and Sport published *Data: A new direction*. This consultation paper proposes a raft of new measures to create a "bold new data regime" and "review and simplify the regulatory landscape … to avoid duplication, overlaps and lack of clarity".[82]

38. Some further potential changes are in prospect. The DCMS consultation, *Data: A new direction,* proposes merging the role of the Biometrics and Surveillance Camera Commissioner into the Information Commissioner's Office. A consultation response from the current Biometrics and Surveillance Camera Commissioner noted that he had not been made aware of this proposal before publication. Professor Fraser Sampson has stated his belief that the consultation was a "formality", with the decision having already been made. He emphasised the need for transparent decision making, which was "particularly acute if public trust is to be maintained in the independent regulation and oversight of police use of biometrics and surveillance." He was strongly against the proposal itself, which he described as "ill-conceived"; "the wrong answer contained within the wrong question"; and "unlikely to produce simpler, stronger governance. It is more likely to result in dilution and further complexity".[83]

39. The appointment of additional bodies may also undermine the ambition to simplify the institutional landscape. In October 2021, the APCC, NPCC, and PDS told us that they were working towards establishing a national Digital and Data Ethics Guidance Group (DDEGG).[84] One month later, Baroness Williams of Trafford told the House of Lords that an NPCC Data Board and a central Data Office within PDS would be established.[85] These three bodies are in addition to ongoing work on a new national governance model inspired by the West Midlands Police Ethics Committee (see Chapter 5).

40. While many plans and strategies exist, they are either limited to police practices, or they address thematic issues, such as data protection. There appears to be a lack of cross-departmental co-ordination, joint working or consultation. While the Minister said that, as a Minister in both the Home Office and the Ministry of Justice, he was the "living embodiment" of cross-departmental working, this does not appear to have impacted strategic

[81] Department for Business, Energy & Industrial Strategy, 'Guidance National AI Strategy' (22 September 2021): https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version [accessed 1 February 2022]

[82] Department for Digital, Culture, Media & Sport, *Data: A new direction*, para 409. See also written evidence from defenddigitalme (NTL0044) and Q 108 (Kit Malthouse MP).

[83] DCMS Consultation: 'Data: A new direction' Response by the Biometrics and Surveillance Camera Commissioner: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1030248/BSCC_DCMS_Consultation_Response.pdf [accessed 1 February 2022]

[84] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049)

[85] HL Deb, 3 November 2021, cols 1301–1305

thinking on the use of new technologies in applying the law, and there is no indication of any collective governmental effort towards a single strategy.[86] On the contrary, there are many indications of siloed thinking. The DCMS consultation, *Data: A new direction*, could have various implications for the use of new technologies in the application of the law, including in policing, but makes very little reference to either. Similarly, BEIS and DCMS are collectively responsible for the implementation of the *National AI Strategy*, which focuses on businesses and the benefits of innovation and does not appear to have considered the needs of the Ministry of Justice or the Home Office at any length, or AI's potential in their sectors. The Minister for Crime and Policing had little to say on the strategy, or on the upcoming governance White Paper.

41. **We have heard no evidence that the Government has taken a cross-departmental strategic approach to the use of new technologies in the application of the law. There appears in practical terms to be a considerable disconnect across Government, exemplified by confusing and duplicative institutional oversight arrangements and resulting in a lack of coordination. Recent attempts to harmonise have instead further complicated an already crowded institutional landscape. Thorough review across Departments is urgently required.**

42. ***We recommend that the Government rationalise the respective roles of Departments as they pertain to the use of new technologies in the application of the law.***

43. ***We recommend that the Government conduct a review to rationalise and consolidate governance structures of the use of technologies in the application of the law.***

44. ***As part of rationalisation, the Government should establish a single national body to govern the use of new technologies for the application of the law. The new national body should be independent, established on a statutory basis, and have its own budget. The body would have several functions and responsibilities, which we detail in Chapter 5. It should draw on as wide as possible a range of expertise.***

The legislative framework

A reliance on the Courts

45. We noted a tendency of witnesses to point to the courts to give guidance and set standards. David Tucker, Faculty Lead on Crime and Criminal Justice at the College of Policing, told us:

> "We have seen that where decisions are challenged or doubted cases go to court and affect the way policing operates. The case of Bridges on live facial recognition is a good example. The Appeal Court said that there was an absence of policy, so we are filling that gap and moving to apply these principles to this piece of technology".[87]

[86] Q 100 (Kit Malthouse MP)
[87] Q 89 (David Tucker)

Box 5: The Bridges case and the Public Sector Equality Duty

1. The Public Sector Equality Duty requires public authorities in the exercise of their functions to have due regard to the need to:

   (a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Equality Act 2010;

   (b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;

   (c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.[88]

2. The Bridges case, taken to the Court of Appeal, demonstrates the importance of this duty in connection with the deployment of new technologies. Mr Edward Bridges, a civil liberties campaigner, brought a claim against South Wales Police for using live facial recognition technology on a number of grounds, including non-compliance with the public sector equality duty. The Court of Appeal found that South Wales Police had failed to do all that it could reasonably do to fulfil the duty in respect of its use of live automated facial recognition and establish whether the technology might be biased.

3. The judgment included the observation: "We would hope that, as [Automated Facial Recognition] is a novel and controversial technology, all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias."[89]

46. When we asked the Minister about evaluation mechanisms to test whether technologies worked, he told us that technologies were evolving, and guidelines with them. When posed the possibility that a lack of evaluation might be causing injustice, he responded:

> "Do not forget that all this stuff is testable in court. As you will have seen, the live facial recognition that South Wales Police use underwent judicial review and was tested in court. That is how we test those uncertainties … by testing them in front of a judge."[90]

47. Alun Michael, Police and Crime Commissioner for South Wales and Joint Lead for Data and Bioethics at the Association of Police and Crime Commissioners, made a crucial point. He told us that questions of ethics: what was acceptable to use and for what purpose, was not of interest to the courts. He said that the courts are "not interested in any of that—they [are] interested in whether it was legal."[91]

48. The Court is an appropriate forum to determine if a law has been broken—or, through judicial review, to analyse if a decision was lawful. This does happen—the witnesses above were referring to the Bridges Case (see Box 5).

[88] Ministry of Justice, *Public sector equality duty* (6 July 2021): https://www.gov.uk/government/publications/public-sector-equality-duty [accessed 4 February 2022]

[89] Royal Court of Justice, *R v The Chief Constable of South Wales Police*, [2020] EWCA Civ 1058

[90] Q 110 (Kit Malthouse MP)

[91] Q 92 (Alun Michael)

We have also been told that both domestic courts and the European Court of Human Rights had been relied upon in the past.[92]

49. Neither criminal cases nor judicial reviews are systematic processes: they are specific and rely on cases or applications being brought. They also require extensive resources.

50. **While they play an essential role in addressing breaches of the law, we cannot expect the Courts to set the framework for the deployment of new technologies.**

"A fragmented landscape"

51. It was made clear to us that legislation around the use of new technologies is very limited. NCC Group told us that "there is very little legislation and regulation overseeing the safe and secure rollout of [Artificial Intelligence] and [Machine Learning]-based technologies."[93] The Bar Council agreed: "For some technologies, such as AI, it is not clear that there is an effective existing legal framework."[94] It was also clear that the framework is "fragmented".[95] Archie Drake and Perry Keller identified four related bodies of law applicable to the use of technologies in the application of the law: human rights, data protection, discrimination, and public administration.[96] Written evidence from the Home Office elaborated:

> "The framework includes police common law powers to prevent and detect crime, the Data Protection Act 2018, Human Rights Act 1998, Equality Act 2010, the Police and Criminal Evidence Act 1984 (PACE), the Protection of Freedoms Act 2012 (POFA), and law enforcement bodies' own published policies."[97]

52. Our evidence reflected organisational confusion about what guidance, regulation and legislation applied. With regard to procurement, a former police officer told us that forces "lack confidence about compliance with regulation."[98] The NCC group stated that organisations are confused about where to find guidance, and what standards should be met. They told us that "the plethora of available resources, studies and research" makes it difficult "for organisations to understand what authoritative sources of guidance and information they should follow."[99]

Calls for strengthened legal framework

53. There is no specific legislative basis for the use of technologies in the application of the law. Several contributors argued that the risks inherent in the use of advanced technologies were so severe that a stronger statutory basis was required. As Dr David Leslie, Ethics Theme Lead at the Alan Turing Institute, told us, and as we indicate throughout this report, "there are additional ethical questions and issues of collective rights involved."[100] The Public Law Project recommended exploring "options along the lines

[92] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)
[93] Written evidence from NCC Group (NTL0005)
[94] Written evidence from the Bar Council (NTL0048)
[95] Written evidence from NCC Group (NTL0005)
[96] Written evidence from Archie Drake and Perry Keller (NTL0011)
[97] Written evidence from the Home Office (NTL0055)
[98] Q 73 (David Lewis)
[99] Written evidence from NCC Group (NTL0005)
[100] Q 36 (Dr David Leslie)

of the EU Commission's proposed AI regulation" (see Box 6). [101] Professor Pete Fussey and his co-contributors called for dedicated legislation, arguing for a specific legal basis.[102] It was their view that "public policies or codes of practice cannot be substituted for legislation."[103]

54. It was felt that clarifying and strengthening the legal framework around new technologies in the application of the law would enable positive uses of technology to "flourish". Robin Allen QC and Dee Masters argued that "public actors and private companies need clear, pragmatic and effective regulatory frameworks because it provides a safety net within which 'good' AI can be developed whilst also protecting the fundamental rights of the public."[104] Archie Drake and Perry Keller had a similar view, stating that "legal uncertainty tends to harm business and innovation as well as public trust in the criminal justice system (and technology)."[105] In a joint submission, three police bodies wrote that "Government should seek to clarify public appetite for new technologies and legislate so that policing has a clearer basis on which to make policies and decisions about deployment."[106]

55. It was pointed out that legislation would bring strength and a level of protection which guidance documents could not. Professor Sandra Wachter, Associate Professor at the University of Oxford, thought that "soft regulation would be irresponsible" because the criminal justice system is "one of the most high-risk areas [she] can think of".[107] Dr Joe Purshouse and his co-contributors reflected that while guidance documents may be cited in court, they "do not provide actionable grounds for an individual to make a complaint", adding that "non-compliance would not impact on the admissibility of any material gleaned."[108]

[101] Written evidence from Public Law Project (NTL0046)

[102] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)

[103] *Ibid.*

[104] Written evidence from Robin Allen QC and Dee Masters (NTL0019)

[105] Written evidence from Archie Drake and Perry Keller (NTL0011)

[106] Written evidence from the Association of Police and Crime Commissioners (APCC), National Police Chiefs' Council (NPCC), and Police Digital Service (PDS) (NTL0049)

[107] Q 73 (Dr Liam Owens and Professor Sandra Wachter)

[108] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021)

Box 6: The EU Artificial Intelligence Regulation Proposal

1. At the time of writing, the Council of the European Union is considering a draft Regulation on Artificial Intelligence brought forward by the Commission in April 2021. (The Slovenian Presidency proposed a compromise text on 29 November 2021.)[109] The proposal is intended to achieve the following objectives:

- ensure that AI systems used, and placed on the EU Single Market. are safe and respect existing law on fundamental rights and EU values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; and
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

2. To achieve these objectives, a four-tiered risk framework is proposed based on a system's intended purpose, from "minimal or no risk" to "unacceptable risk". The proposal notably foresees the establishment of a public register of "high-risk AI systems" and the appointment by Member States of a national competent authority to enforce the regulation.

Source: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts (COM(2021) 206 final)

A balanced approach

56. Concern was expressed that regulation may be impractical, particularly if it targeted emerging technologies before deployment. One developer was concerned about the ability of legislators to match the pace of development, saying: "I do not know how easy it would be to create a guideline for something so leading-edge and so very new."[110] The Minister explained this view further:

> "This stuff is coming so fast that it is hard for legislators to keep up. We prefer to produce a set of principles and then, as technology appears and is put to use, to work out what is happening and govern it through guidelines and the transparency structures that we have talked about."[111]

The Serious Fraud Office thought that "Delays to updating legislation and/or guidance may hamper the application of new technology."[112] We take these concerns seriously, and note the danger of delays, as well as the danger that hugely detailed or otherwise overly onerous statute may "stifle innovation".[113]

57. We note the views of witnesses who thought that the proposed EU Artificial Intelligence Regulation was likely to become a global model for regulation.[114] We agree with David Lewis, former Deputy Chief Constable, and ethics lead

[109] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 14278/21 [accessed 24 February 2022]

[110] Q 75 (Dr Liam Owens)

[111] Q 109 (Kit Malthouse MP)

[112] Written evidence from the Serious Fraud Office (NTL0034)

[113] Written evidence from BAE Systems (NTL0056)

[114] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035), Q 73 (David Lewis), see also written evidence from BAE Systems (NTL0056).

of the National Police Chiefs' Council, who, among others, thought that any new legal framework should be adopted at national level, but that "it would be helpful if it was not too divergent from international regulation".[115]

The practicalities

58. Our evidence leaned towards strengthening the legal framework. However, there was general uncertainty of the form that this could take. While there were some (varied) suggestions, the NCC Group was representative of the evidence received when it said that it "would support further reviews into what regulatory and legal levers might be used to ensure organisations developing and using AI/ML are taking the appropriate steps."[116]

Box 7: Types of legislation

- An Act of Parliament ('primary legislation') is law made by Parliament.
- A Statutory Instrument ('SI', 'secondary legislation') is proposed by the Government under powers given by an Act of Parliament. Different SIs are subject to different levels of Parliamentary involvement. They may be debated but cannot be amended by Parliament and it is extremely rare for Parliament to prevent an SI from being passed. They are relatively quick and easy for the Government to pass and amend.
- 'Statute' is made by Parliament, both primary and secondary legislation.
- Statutory regulations are made by an SI, and so subject to SI procedures. Non-statutory regulations are not subject to Parliamentary procedure.
- Guidance, which is not binding, sets out matters to which regard should be had—'what you should do'.

59. Some contributors were detailed about what should be set out in legislation. One contribution listed, for example, the circumstances in which a new technology may be used, the framework for authorising a deployment, and the supervisory and accountability mechanisms.[117]

60. Others favoured a value- and principles-based approach, with Alun Michael saying that "the values and principles need to be established in law".[118] As our witnesses pointed out, "certain things with AI will always be the same … we will always have a data issue, a bias issue and an explainability issue."[119] Professor Raab similarly told us that among the "plethora" of guidance, research and reviews, a consensus had emerged on some principles: "privacy protection, accountability, fairness, non-discrimination, justice, transparency, safety and cybersecurity, serving the common good, explainability, and human oversight".[120] As we highlighted in paragraph 56, the Minister himself said that the Government's preferred approach was to produce a set of principles—our view is that these should be translated into statute. The Government has already endorsed the principles on Artificial Intelligence agreed by the Organisation for Economic Co-operation and Development (OECD), in the absence of a concrete set of relevant principles from Government, perhaps these would be suitable (see Box 8). We

[115] Q 73 (David Lewis)
[116] Written evidence from NCC Group (NTL0005)
[117] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)
[118] Q 98 (Alun Michael)
[119] Q 69 (Professor Sandra Wachter)
[120] Written evidence from Professor Charles Raab (NTL0014)

acknowledge the demands that the development of new legislation would place on parliamentary time and Government capacity, and that legislation is not a 'quick fix'. We strongly believe, however, that the risks are such that specific statute for the use of technologies in the application of the law is required. Statute would also help to facilitate consistency of which principle applies in which context.

Box 8: The OECD principles for responsible stewardship of trustworthy AI

In May 2019, the Organisation for Economic Co-operation and Development, of which the UK is a member, adopted a recommendation on Artificial Intelligence. While the UK endorsed this recommendation, it is not legally binding. It outlined the following principles for responsible stewardship of trustworthy AI:

- Inclusive growth, sustainable development and well-being;
- Human-centred values and fairness;
- Transparency and explainability;
- Robustness, security and safety;
- Accountability.

Source: OECD Legal Instruments, 'Recommendation of the Council on Artificial Intelligence' (22 May 2019): https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [accessed 3 February 2022]

61. **Given the potential costs of technologies and the problems that can and do arise from their implementation, including with respect to privacy rights, freedoms, and discrimination, we consider that a stronger legal framework is required to prevent damage to the rule of law.**

62. Value- and principles-based statute would also provide a framework for lower-level regulation. We heard that there is an absence of overarching "formal policing-specific regulation on the use of data capabilities" in general.[121] While regulations issued through statutory instruments receive little scrutiny through Parliament, this does mean that they can be more dynamic.

63. Professor Raab highlighted an important danger—that "inventories of high-level principles court irrelevance in the law-enforcement field if less attention is paid to how they may be implemented in practice."[122] To address this danger, several witnesses called for regulation to "minimum security standards".[123] The NCC Group agreed and called for "appropriate regulation that mandates a minimum approach."[124] Our witnesses were divided on how detailed regulations should be, and there was no consensus on whether they should be sector-specific, or cross-sectoral.[125]

[121] Written evidence from Dr Jamie Grace (NTL0001)

[122] Written evidence from Professor Charles Raab (NTL0014)

[123] Written evidence from NCC Group (NTL0005)

[124] *Ibid.*

[125] For an example of those advocating a sector-specific regulatory approach, see Q 43 (Dr Rosamunde van Brakel); for an example of those advocating cross-sector approach, see Q 15 (Professor Charles Raab).

64. In Chapter 5, we discuss an absence of minimum standards to which advanced technologies are held. It is our strong view that appropriate standards should be implemented, and that they be transposed into regulations.

65. ***We recommend that the Government bring forward primary legislation which embodies general principles, and which is supported by detailed regulations setting minimum standards. We consider that this approach would strike the right balance between concerns that an overly prescriptive law could stifle innovation and the need to ensure safe and ethical use of technologies.***

66. ***Along with 41 other countries, the Government has endorsed principles of Artificial Intelligence. In response to this report, the Government should outline proposals to establish these firmly in statute.***

Guidance

67. Evidence on guidance was less contentious than calls for legislation. There were three problems identified with guidance as it currently stands: that it is difficult to know which applies; that there are gaps; and that it does not always assist in practice. Crucially, it is only guidance.

68. There is plenty available. The Home Office told us about guidance on the CAID programme (the Child Abuse Image Database, a facial recognition tool which helps identify victims and offenders)[126], while guidance on facial recognition is currently being developed by the College of Policing, and the Ministry of Justice is working with the Alan Turing Institute to extend existing guidance on the use of data-driven technologies within the justice system.[127] There is also various guidance available from the Surveillance Camera and Information Commissioners[128], and a host of guidance from non-governmental sources such as the ALGO-care framework (a practical decision-making framework for the policing context).[129] The Metropolitan Police Service noted that the application of the "variety of guidance, opinion, codes, directions and proposals for ethical frameworks … risks confusion and inconsistency".[130]

[126] Written evidence from the Home Office (NTL0055)

[127] College of Policing, 'Police use of live facial recognition technology—have your say' (17 May 2021): https://www.college.police.uk/article/police-use-live-facial-recognition-technology-have-your-say [accessed 26 January 2022] and written evidence from the Ministry of Justice (NTL0053)

[128] Information Commissioner's Office, 'Guidance index': https://ico.org.uk/for-organisations/guidance-index/ and Biometrics and Surveillance Camera Commissioner, 'Surveillance camera guidance, tools and templates' (22 October 2018): https://www.gov.uk/government/collections/surveillance-camera-guidance-tools-and-templates [accessed 7 February 2022]

[129] Marion Oswald, 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality', *Information & Communications Technology Law*, vol.27, (3 April 2018): https://www.tandfonline.com/doi/full/10.1080/13600834.2018.1458455 [accessed 7 February 2022]

[130] Written evidence from the Metropolitan Police Service (NTL0031)

Box 9: Application of the Equality Act 2010

- To illustrate the confusion in the application of law, several submissions referred to the Equality Act 2010. For instance, Archie Drake and Perry Keller told us that "authorities have struggled to implement new technologies in ways that comply with the Equality Act 2010 including the Public Sector Equality Duty".[131]
- Robin Allen QC and Dee Masters noted a lack of guidance on how the Act could be applied, saying: "there has been no guidance from the Government concerning how the Equality Act 2010 regulates AI in any detailed way … there has been very little by way of detailed analysis of how the Equality Act 2010 actually applies to algorithmic decision making."[132]
- In late 2020, the Centre for Data Ethics and Innovation called for Government to issue guidance that clarifies the Equality Act responsibilities of organisations using algorithmic decision-making. This, they said, should include guidance on the collection of protected characteristics data to measure bias and the lawfulness of bias.[133]

69. It was clear, though, that there were gaps. One submission told us that "many technologies are adopted without guiding codes of practice setting out consistent and appropriate use." The same contributors told us that:

> "The absence of clear guidance and oversight created significant dilemmas for [those] officers. In particular, officers became responsible for continuously evaluating the applicability of any analogous guidance, which added to the strain of using such tools and engendered highly inconsistent practices."[134]

70. Contributors also told us that where guidance is available, it is not necessarily useful in practice. Professor Charles Raab, for example, argued that the "circumstances of using the device" can "bring principle and practice together, often in some tension." He went on to tell us that "there is no tidy inventory of ethical principles … across the welter of frameworks and lists".[135] Robin Allen QC and Dee Masters recommended "practical guides on how to ensure that technology is used appropriately".[136] While the College of Policing is responsible for producing Authorised Professional Practice, this does not appear to have a focus on the use of particular types of technologies.[137]

71. Some contributors were concerned that "delays to updating legislation and/ or guidance may hamper the application of new technology".[138] As with training (see Chapter 3), this perceived risk is based on an assumption that all guidance would have to be complete and comprehensive before deployment. As Professor Raab pointed out, comprehensive and practical guidance on

[131] Written evidence from Archie Drake and Perry Keller (NTL0011)

[132] Cloisters, *In the matter of automated data processing in Government decision making* (7 September 2019): https://www.cloisters.com/wp-content/uploads/2019/10/Open-opinion-pdf-version-1.pdf [accessed 25 January 2022]

[133] Centre for Data Ethics and Innovation, *Review into bias in algorithmic decision-making* (November 2020), p 12: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf [accessed 2 February 2022]

[134] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)

[135] Written evidence from Professor Charles Raab (NTL0014)

[136] Written evidence from Robin Allen QC and Dee Masters (NTL0019)

[137] College of Policing, 'APP content' (4 November 2015): https://www.app.college.police.uk/app-content/ [accessed 4 February 2022]

[138] Written evidence from the Serious Fraud Office (NTL0034)

the use of types of technologies will require consistent review and ongoing updates as tools are used in operational settings, and practical operational issues identified.[139] It could not therefore be expected that such guidance will ever tackle all of the specificities of particular tools. Issuing it and updating it on an ongoing basis is far more practicable than awaiting a day that it is 'complete'—and would certainly be a marked improvement on the current position.

72. BAE Systems thought that it was worth considering "whether the various frameworks and guidelines could be drawn together into a single supplier Code of Practice."[140] This approach, however, could not address the important practical and standards-based questions which arise from the use of particular technologies.[141]

73. The National Police Chiefs' Council are establishing a national Digital and Data Ethics Guidance group to "provide national support, particularly on complex cases."[142] As it stands, however, there is no one place where guidance on the use of new technologies can be found, and, as far as we are aware, no clear requirement on Police bodies to produce it.

74. ***Guidance, both general and specific, is urgently needed. The Government should require that national guidance for the use of advanced technological tools in policing and criminal justice is drawn up and, as part of their response to this report, should outline concrete plans for this.***

75. ***There is a need for a 'one-stop shop' collating all relevant legislation, regulation and guidance and drawing together high-level principles with practical user guides. This collation should be updated by the College of Policing on an ongoing basis, and direct users to the guidance and regulation relevant to their circumstance and need.***

Accountability

76. Our witnesses were clear that accountability is an essential principle in this sphere. The Law Society of England and Wales told us that it is "vital that systems and the people who develop them should be … accountable",[143] with academics from the University of Essex agreeing that supervisory and accountability mechanisms were needed "to avoid arbitrary rights interferences".[144]

77. Trust was often put forward as the main benefit of accountability. BAE systems referred to the need for technology users to "be accountable for decisions in order to support public trust."[145] The Information Commissioner's Office were clear that, "human oversight remains a fundamental factor in appropriating responsibility and retaining trust in new technologies and the sectors that use them."[146] For public bodies and the police, with "vital public service responsibilities", "unmatched powers over citizens, and their

[139] Written evidence from Professor Charles Raab (NTL0014)

[140] Written evidence from BAE Systems (NTL0056)

[141] We consider standards in depth in Chapter 5.

[142] Written evidence from the Association of Police and Crime Commissioners, National Police Chiefs' Council, and Police Digital Service (NTL0049)

[143] Written evidence from the Law Society of England and Wales (NTL0023)

[144] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)

[145] Written evidence from BAE Systems (NTL0056)

[146] Written evidence from the Information Commissioner's Office (NTL0016)

potential influence on individuals, groups and society"[147], this trust is critical. We would add that the Nolan Principles of public life require decisions to be taken impartially, fairly and on merit, and that holders of public office are accountable to the public for their decisions and actions.[148]

78. Accountability was defined in moral, political, and legal terms. The Public Law Project combined the three, telling us that accountability encompasses: "responsibility" (who can be "praised, blamed, and sanctioned"); "answerability", (who can be called to explain decisions); and "sanctionability" (subject to sanctions ranging from "social opprobrium to legal remedies").[149]

79. Contributors acknowledged failure as an important part of progress. Dr Liam Owens, Founder and CEO of technology provider Semantics 21 stated that "we need to evolve and take the chance of engaging with AI and engaging with new technologies." This is why, he told us, it is important to "give it a go … if it does not work no one should be held accountable."[150] Although Dr Owens subsequently concluded that "there has to be accountability"[151], the Minister seemed to share his view on the need to create space for failure. Kit Malthouse MP said that forces must be allowed to fail "before we jump on everything." It is important to note that the Minister was speaking in this context about technology which proves "not to be terribly useful"[152], rather than about a failure to comply with minimum standards or where a miscarriage of justice had occurred.

80. Privacy International argued that clearly defined responsibilities across actors involved in the deployment of a given technology was an essential tenet of accountability.[153] (Technologies are not moral agents, and cannot be held accountable.[154]) When we asked our witnesses who was ultimately accountable for the use or misuse of technology in the context of the application of the law, no clear answer emerged. Variously accountable were:

- **Ministers**. The Bar Council told us that "final accountability currently lies with Ministers and the executives providing oversight".[155] Academics from King's College London similarly considered that "accountability arrangements need to start at ministerial levels". In particular, they thought that the Home Secretary, the Lord Chancellor and Secretary of State for Justice, and the Minister for Crime and Policing should be answerable for "how the Government's vision of technological change in the system safeguards its effectiveness and legitimacy."[156] The Minister for Crime and Policing agreed that he, and Government as a whole, are "broadly—whether [they] like it or not—responsible for most things."[157]

[147] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)

[148] Committee on Standards in Public Life, 'The Seven Principles of Public Life' (31 May 1995): https://www.gov.uk/government/publications/the-7-principles-of-public-life/the-7-principles-of-public-life--2 [accessed 27 January 2022]

[149] Written evidence from Public Law Project (NTL0046)

[150] Q 72 (Dr Liam Owens)

[151] Q 76 (Dr Liam Owens)

[152] Q 106 (Kit Malthouse MP)

[153] Written evidence from Privacy International (NTL0051)

[154] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040) and Q 31 (Professor Michael Wooldridge)

[155] Written evidence from the Bar Council (NTL0048)

[156] Written evidence from Archie Drake and Perry Keller (NTL0011)

[157] Q 107 (Kit Malthouse MP)

- **Chief Constables**. We were told that "Chief Constables are responsible for the operational deployment of new technologies".[158] Chief Constables are held accountable by the Police and Crime Commissioners (PCCs), who were described by one PCC as "constantly inquisitive and challenging."[159]

- **Technology suppliers**. Some of our witnesses believed that "ultimately, technology producers and users should be accountable for new technologies".[160] Dr Leslie argued that "accountability entails that designers and implementers are answerable for the parts they play across the entire design and deployment workflow."[161] A developer agreed: "we have to be held accountable for our accuracy"[162] and that "technology providers need to ensure that their products are secure and should take steps to minimise bias", in line with the Government's "Secure by Design approach".[163] Accountability and indeed liability would have to be built into contracts; we have not had the opportunity of examining any forms of contract in use.

- **End users**. It was felt that "users retain a level of responsibility to familiarise themselves with the [technological] solutions" and "should understand the limits of what can be achieved through the use of these technologies".[164] To achieve this, the Bar Council argued for "a properly qualified team dedicated to the oversight of the adoption of any new technology" within every organisation using technology[165], and a group of academics similarly stressed that adopting technology "requires specialist staff to be accountable for the whole system, including algorithms, workflow design, delegation of tasks to humans etc."[166]

In the view of several witnesses, supplier and user accountability were deeply intertwined. NCC Group told us that "both the provider and the end-user should be accountable for the use of AI/ML-based technologies".[167] BAE Systems conceded that "detailed accountability for mistakes is probably shared between purchaser and supplier."[168] Similarly, we heard that "producers should be open and clear about the performance and limitations of their systems" and "should work closely with user communities to ensure technology is fit for purpose at both the testing phase and in operational deployment."[169]

81. Given the variety of actors named as being accountable, we are seriously concerned that this leads to a lack of recourse for people who may suffer from the deployment of advanced technologies. It is to this we now turn.

[158] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049), Q 91 (David Tucker) and Q 90 (Alun Michael)

[159] Q 90 (Alun Michael)

[160] Written evidence from Dr Christopher Lawless (NTL0029)

[161] Q 36 (Dr David Leslie)

[162] Q 76 (Dr Liam Owens)

[163] Written evidence from NCC Group (NTL0005)

[164] *Ibid.*

[165] Written evidence from the Bar Council (NTL0048)

[166] Written evidence from Dr David White *et al.* (NTL0012)

[167] Written evidence from NCC Group (NTL0005)

[168] Written evidence from BAE Systems (NTL0056)

[169] Written evidence from Dr Christopher Lawless (NTL0029)

Lack of recourse

82. The lack of clarity in accountable and responsible individuals and entities was reflected in a confused process for recourse. Various witnesses referred to the courts as a mechanism for accountability[170] Courts can review the use of tools in various ways including judicial review and rulings on the admissibility of evidence. Suggestions of an over-reliance on the courts to rule on the use of new technologies have been discussed in paragraphs 45–50, but the crucial point to emphasise is that they can only do so, or conduct judicial reviews, if a case or challenge is brought to them, with all the requirements on individuals and resources that that entails. The role of courts in society is of course vital, but they are not a substitute for robust accountability mechanisms.

83. Darryl Preston, who is the Police and Crime Commissioner for Cambridgeshire and Peterborough and the Joint Lead for Data and Bioethics at the Association of Police and Crime Commissioners pointed out "the usual complaints procedures" that would be followed if an individual wished to hold their local police force to account.[171] We tested this by asking the Independent Office for Police Conduct (IOPC) whether it held, or had held, any cases relevant to the use of new technologies in the application of the law. They did not.[172] We are grateful for the IOPC's assistance in this matter and note that it is not the only mechanism for complaints against officers or forces. The lack of complaints to this body suggests, though, that complaints mechanisms play a limited role in holding law enforcement to account in their use of advanced technologies.

84. **There is no clear line of accountability for the misuse or failure of technological solutions used in the application of the law. As a result, no satisfactory recourse mechanisms exist.**

85. ***The Government should appoint a taskforce to produce guidance to ensure that lines of accountability, which may differ depending on circumstances, are consistent across England and Wales. The taskforce should act transparently and consult with all affected parties.***

Moratoria

86. Several witnesses called for 'red lines'. Robin Allen QC and Dee Masters stated that algorithms which discriminated in relation to protected characteristics[173] should never be deployed, and that establishing and protecting such redlines would "create trust which in turn allows good uses of technology to flourish."[174] Liberty and Big Brother Watch agreed that some technology could never be safely used, with particular regard to live facial recognition.[175] Archie Drake and Perry Keller thought it "appropriate"

[170] Q 110 (Kit Malthouse MP)

[171] Q 89 (Darryl Preston)

[172] Written evidence from the Independent Office for Police Conduct (NTL0054)

[173] The Equality Act 2010 makes it illegal to discriminate against anyone because of nine characteristics: age; gender reassignment; marriage or civil partnership status; pregnancy or being on maternity leave; disability; race (including colour, nationality, ethnic or national origin); religion or belief; sex; and sexual orientation. These are called 'protected characteristics'.

[174] Written evidence from Robin Allen QC and Dee Masters (NTL0019)

[175] Written evidence from Liberty (NTL0020) and Big Brother Watch (NTL0037)

to ban "clearly harmful or high-risk applications of technology" which lack robust accountability arrangements.[176]

87. We note strong resistance to calls for moratoria. Law enforcement bodies in particular were concerned that "to declare technologies as being 'off limits' to policing risks denying law enforcement the tools it needs to keep the public safe whilst leaving these tools easily available for criminals and commercial users to consume and exploit".[177] On the other hand, we note that the proposed EU AI Regulation would ban systems that pose an 'unacceptable risk', such as social scoring and many deployments of facial recognition technology. The European Parliament has even adopted a non-binding resolution that police forces should be banned from using facial recognition and predictive policing algorithms.[178] UN High Commissioner for Human Rights Michelle Bachelet has also called for "a moratorium on the sale and use of artificial intelligence systems that pose a serious risk to human rights."[179]

88. Moratoria on specific tools, or specific types of tools, do not seem to us to be the most appropriate way of ensuring that a tool is being used appropriately; particularly since such bans could create problems for law enforcement in very serious criminal cases where they may be appropriate. We are keen, though, that as technology develops, the Government should be ready and willing to ban certain tools should it be necessary.

89. ***Moratoria are important and powerful mechanisms. In its response to this report, the Government should set out the circumstances in which it would be willing to deploy them in the future. The new national body we recommend should be empowered to refuse certification for a new tool under those circumstances.***

[176] Written evidence from Archie Drake and Perry Keller (NTL0011)

[177] Written evidence from the Metropolitan Police Service (NTL0031)

[178] Committee on Civil Liberties, Justice and Home Affairs, *Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (13 July 2021): https://www.europarl.europa.eu/doceo/document/A-9-2021–0232_EN.html [accessed 3 February 2022]

[179] United Nations Human Rights Office of the High Commissioner, *Artificial intelligence risks to privacy demand urgent action — Bachelet* (15 September 2021): https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet [accessed 3 February 2022]

CHAPTER 3: TRANSPARENCY

90. Transparency, namely the public disclosure of what technology is currently being used, where, and for what purpose, is key to enable the sound deployment of technological solutions. In this chapter we focus on the importance and current lack of transparency, and proposals to increase it, including to establish a public register of algorithms.[180]

Transparency matters

91. Some saw "intrinsic value" in transparency, referring to the principle of "openness" that forms part of the seven Nolan Principles of public life.[181] David Lewis, for instance, told us that "it is really important to be transparent and open for the public to be able to see what is being used."[182] The Law Society of England and Wales went even further, describing transparency as "vital" and "crucial". Others emphasised the role of transparency in achieving public trust in policing.[183] We heard from the Metropolitan Police Service that transparency is "crucial to effective community engagement when considering if and how to use technology"[184], while the Public Law Project told us that it "allows for proper debate and consensus-building around the use of new technologies in the public interest".[185]

92. Transparency is also important in equalities considerations. Robin Allen QC and Dee Masters told the Committee that "a lack of transparency around the use and application of these technologies is particularly problematic when it comes to assessing any equality implications."[186] Other witnesses pointed out that transparency can play a role in the guarantee of individual rights, especially when technology is applied to individual cases. As Professor Sandra Wachter put it, "the public have a right to know if algorithms are being used to send them to prison".[187] The Bar Council told us that technologies should be "transparent and trustable and ethically designed so as not to deny individual autonomy, recourse and legitimate rights".[188]

93. Evaluation is not possible without transparency. The Public Law Project told us that a lack of transparency around the technology used for the application of the law was "a major challenge" when trying to evaluate technological solutions.[189] Professor Karen Yeung concurred that difficulty in accessing data "is a serious problem for academic researchers"[190], and other contributors added that "transparency is important not only insofar as enabling evaluation

[180] Transparency should be distinguished from explainability, another key concept dealt with in Chapter 4.
[181] Written evidence from Dr Arianna Andreangeli (NTL0038) and (NTL0039)
[182] Q 78 (David Lewis)
[183] Written evidence from Professor Charles Raab (NTL0014), Q 10 (Professor Charles Raab) and Q 98 (Alun Michael). Witnesses were usually referring to the 1829 Peelian principles, see Home Office, *FOI release Definition of policing by consent,* (10 December 2012): https://www.gov.uk/government/publications/policing-by-consent/definition-of-policing-by-consent [accessed 3 February 2022].
[184] Written evidence from the Metropolitan Police Service (NTL0031), see also written evidence from Archie Drake and Perry Keller (NTL0011) and Dr Matthias Wienroth *et al.* (NTL0022)
[185] Written evidence from Public Law Project (NTL0046), see also written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021)
[186] Written evidence from Robin Allen QC and Dee Masters (NTL0019), see also Q 65 (Peter Dawson)
[187] Q 78 (Professor Sandra Wachter)
[188] Written evidence from The Bar Council (NTL0048)
[189] Written evidence from Public Law Project (NTL0046)
[190] Q 57 (Professor Karen Yeung)

of particular technologies but also for ensuring that the decision-making process for the use of technology is open to public scrutiny."[191]

94. ***One of the principles in the new statute we recommend should be transparency.***

A current lack of transparency

95. The Home Office told us that they were "supporting law enforcement organisations to address … the need for transparency",[192] and that "policing is committed to being transparent."[193] The Ministry of Justice also informed us about an annual review of "analytical algorithms—only a small subset of [which] involve data and decisions about individuals". Nevertheless, we ourselves faced difficulties accessing first-hand information, with repeated reference to confidentiality concerns. It is also illuminating that many of the examples we were presented with in our evidence arose from Freedom of Information requests and were not routinely published.

96. On the most basic level, we cannot be certain what technologies are being used for the application of the law in England and Wales. Indeed, Dr Miri Zilka and Dr Adrian Weller from the University of Cambridge, together with Detective Sergeant Laurence Cartwright from Sussex Police, told us that "transparent information about these tools, their purpose, how they are used and by whom is difficult to obtain", adding that "even when information is available, it is often insufficient to enable satisfactory evaluation."[194] The Public Law Project agreed: "it is often difficult to find out about the existence of an [Automated Decision Making] system, let alone getting an explanation of how it works—both in general and in application to a specific individual."[195] It was also felt that this confusion extended to regulators: Dee Masters and Robin Allen QC had "become increasingly aware of the lack of understanding by regulators and the general public of the way in which AI systems are being used in their field of activity."[196]

97. The current lack of transparency may be partly explained on operational grounds. The Metropolitan Police Service pointed to "rare" occasions where they would want to "guard its particular use of some technologies carefully in order to preserve their effectiveness."[197] While we accept that there can be serious difficulties around releasing sensitive information, their suggestion to institute guiding principles within a code of practice would not provide the assurance of transparency that is required to ensure scrutiny and engender trust.

98. **There are no systematic obligations on individual departments, public bodies, and police forces to disclose information on their use of advanced technological solutions. It is impossible for Parliament, press, academia, those responsible for procurement and—importantly—those subject to their use to scrutinise and challenge**

[191] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021), see also written evidence from Privacy International (NTL0051)

[192] Written evidence from the Home Office (NTL0055)

[193] *Ibid.*

[194] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)

[195] Written evidence from Public Law Project (NTL0046), see also written evidence from Dr David White *et al.* (NTL0012) for a specific example.

[196] Written evidence from Robin Allen QC and Dee Masters (NTL0019)

[197] Written evidence from the Metropolitan Police Service (NTL0031)

the use of technological solutions as they cannot know who is using what, for how long, for what purpose, or with what safeguards. This risks undermining trust in the police, the justice system, and the rule of law.

A duty of candour

99. It was suggested that an initial step to achieving greater transparency would be a public administration "duty of candour".[198] As it stands, there is no statutory duty of candour on the police. Duty of candour obligations apply largely in health care settings and the relevant legislation sets out some specific requirements to be followed when things go wrong; including informing people about the incident, providing reasonable support, providing truthful information, and an apology.[199]

100. A recent review of the Daniel Morgan case reported a number of failings in the police handling of the case. It recommended: "the creation of a statutory duty of candour, to be owed by all law enforcement agencies to those whom they serve, subject to protection of national security and relevant data protection legislation."[200] Proposals from families bereaved by the Hillsborough disaster[201] have also argued for a statutory duty of candour. The House of Lords supported an amendment to the Police, Crime, Sentencing and Courts Bill that would introduce one, but this option was not pursued by the Government.[202]

101. There are valuable lessons to be learned when tools have been found to be unsuitable or have been withdrawn. Sharing that information widely would allow others to avoid repeating mistakes, but we do not see this information being shared. The Durham Harm Assessment Risk Tool (a predictor for reoffending rates, discussed in more depth in paragraph 127), was withdrawn in September 2020. A study into the effectiveness of this tool has produced some headline figures into the accuracy of forecasting, but publicly available information about why the tool was withdrawn is limited to one short sentence in a policing publication:

> "Following the completion of the research project, Durham Constabulary stopped using Hart in September 2020 due to the resources required

[198] Written evidence from Archie Drake and Perry Keller (NTL0011)

[199] Public Health England, *Guidance Duty of Candour,* (5 October 2020): https://www.gov.uk/government/publications/nhs-screening-programmes-duty-of-candour/duty-of-candour [accessed 24 February 2022]

[200] An independent review found that there had been systemic failings in the Metropolitan Police's handling of the death of Daniel Morgan in 1987. See Daniel Morgan Independent Panel, *The Report of the Daniel Morgan Independent Panel,* p 1116: https://www.danielmorganpanel.independent.gov.uk/wp-content/uploads/2021/06/CCS0220047602–001_Daniel_Morgan_Report_Volume_3.pdf [accessed 5 February 2022]

[201] In 2017, a report from the Right Reverend James Jones into the experiences of the families bereaved due to the Hillsborough disaster called for a statutory duty of candour to apply to police officers. This proposal has been called the 'Hillsborough Law'. See The Right Reverend James Jones KBE, *'The patronising disposition of unaccountable power'. A report to ensure the pain and suffering of the Hillsborough families is not repeated*, (1 November 2017) p 8: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/656130/6_3860_HO_Hillsborough_Report_2017_FINAL_updated.pdf [accessed 5 February 2022]

[202] HL Deb, 22 June 2021, cols 134–136, see also HL Deb, 17 January 2022, cols 1357–1362 and Police, Crime, Sentencing and Courts Bill amendment 114C.

> to constantly refine and refresh the model to comply with appropriate ethical and legal oversight and governance."[203]

While the full study is expected to be published (at a date yet to be confirmed), there are no commitments as to what information it will contain.

102. ***We urge the Government to consider what level of candour would be appropriate to require of police forces regarding their use of advanced technologies.***

A register of algorithms

103. Establishing a public register of algorithms, similar to the one foreseen in the proposed EU AI Regulation (see Box 6), was convincingly portrayed by many witnesses as the ideal mechanism by which transparency could be achieved.[204] Barristers Robin Allen QC and Dee Masters, for instance, viewed a "public register of algorithms used in relation to the application of the law" as "invaluable".[205] Professor Colin Gavaghan—Director of the New Zealand Law Foundation Centre for Law and Policy in Emerging Technologies at the University of Otago—noted that "the most basic level of transparency relates to knowledge of which new technologies are being used, by whom, and for what purposes", adding that "a regularly maintained and publicly accessible register of algorithms and [Automated Decision Making] systems used by government agencies" could achieve this.[206] This recommendation is one that has previously received strong support (see Box 10).

Box 10: Previous support for a register

- In 2018, the House of Commons Science and Technology Committee recommended that "the Government should produce, publish, and maintain a list of where algorithms with significant impacts are being used within Central Government, along with projects underway or planned for public service algorithms".[207]
- A 2019 report by the Law Society of England and Wales concluded that "a national register of algorithmic systems in the criminal justice system should be created".[208]

[203] Police Professional, 'Artificial intelligence 'marginally better' at predicting re-offending' (25 January 2022): https://www.policeprofessional.com/news/artificial-intelligence-marginally-better-at-predicting-reoffending/ [accessed 24 February 2022]

[204] Q 65 (Silkie Carlo, Peter Dawson, Professor Karen Yeung) and Q 78 (David Lewis, Dr Liam Owens, Professor Sandra Wachter)

[205] Written evidence from Robin Allen QC and Dee Masters (NTL0019)

[206] Written evidence from Professor Colin Gavaghan (NTL0047), see also written evidence from Archie Drake and Perry Keller (NTL0011) and Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035).

[207] Science and Technology Committee, *Algorithms in decision-making* (Fourth Report, Session 2017–2019, HC 351)

[208] Q 11 (Professor Sylvie Delacroix) see also the Law Society of England and Wales, *Algorithm use in the criminal justice system report*, p 66: https://www.lawsociety.org.uk/en/topics/research/algorithm-use-in-the-criminal-justice-system-report [accessed 10 January 2022].

- A 2020 report by the Royal United Services Institute (RUSI) commissioned by the Centre for Data Ethics and Innovation (CDEI) found that "the NPCC and APCC should … maintain a high-level catalogue for all algorithms used by police forces nationwide".[209] David Lewis told us that the NPCC had recently accepted this recommendation, although caveating that "there is a matter of degree to be debated".[210] There is no indication that such a catalogue would be published.
- A 2020 report by the Centre for Data Ethics and Innovation endorsed previous recommendations and suggested a "pilot in a specific part of the public sector".[211]
- In 2021, the Commission for Race and Ethnic Disparities called for the introduction of "a mandatory transparency obligation on all public sector organisations applying algorithms that have an impact on significant decisions affecting individuals".[212] This recommendation was later endorsed by the Independent Office for Police Conduct.[213]

104. This was not a universal view. A number of witnesses cautioned against an over emphasis on transparency. One contributor thought that "it is not always feasible or even desirable to make algorithms in criminal justice fully transparent."[214] In the following paragraphs we examine those arguments.

105. There were concerns that a requirement to log entries into a register could be so burdensome as to prevent smaller organisations from innovating, while the risk of infringement upon a commercial vendor's Intellectual Property rights may disincentivise innovation.[215] BAE Systems would oppose the establishment of a register because it "could damage supplier IP [or] make solutions vulnerable to future criticism (e.g. if the algorithm is superseded by a better one)."[216] This argument was met with scepticism by Professor Sandra Wachter. She told the Committee that "it is very important to differentiate between research and deployment" and argued that research would remain unaffected by a register that applied to commercial products only.[217]

106. We also heard that a register could be hazardous. By sharing too much information about how a system works, some witnesses were concerned third parties could be equipped with the necessary knowledge to manipulate their products. For instance, the information published on a register "could be used to infer how a [Machine Learning] model would make a specific legal decision, and thus what inputs could be crafted to manipulate a desired legal

[209] RUSI, *Data Analytics and Algorithms in Policing in England and Wales* (February 2020), p xi: https://static.rusi.org/rusi_pub_165_2020_01_algorithmic_policing_babuta_final_web_copy.pdf [accessed 21 January 2022]

[210] Q 78 (David Lewis)

[211] Centre for Data Ethics and Innovation, *Review into bias in algorithmic decision making* (November 2020): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf [accessed 21 January 2022]

[212] Commission on Race and Ethnic Disparities, *Independent report, Forward, introduction and full recommendations*, (28 April 2021): https://www.gov.uk/government/publications/the-report-of-the-commission-on-race-and-ethnic-disparities/foreword-introduction-and-full-recommendations#full-recommendations [accessed 10 January 2022]

[213] Written evidence from the Independent Office for Police Conduct (NTL0054)

[214] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)

[215] Q 78 (Dr Liam Owens)

[216] Written evidence from BAE Systems (NTL0056)

[217] Q 78 (Professor Sandra Wachter) and Q 73 (Professor Sandra Wachter)

outcome."[218] Indeed, several witnesses were worried that a technological solution "could be 'gamed' by criminals" if algorithms were published.[219] This is what BAE Systems calls "data poisoning"[220] and the NCC Group calls "adversarial Machine Learning".[221]

107. In addition to confidentiality and security concerns, we heard that a register could be costly to establish. The Committee heard that establishing a register was "a massive task" because of the number of algorithms already in use.[222] A group of legal academics noted that the proposal to introduce a register of "high-risk" algorithms in the EU had sparked "considerable debate" about whether it would "unduly increase the costs of development and deployment of AI systems".[223] Two other witnesses raised the same concerns,[224] which were dismissed by those who contended that "it is neither legal nor ethical to argue that technologies should be implemented if they pose serious risks to human rights and equality, only simply to save money." They suggested that limiting the scope of the register to the most meaningful algorithms would make the endeavour manageable.[225] Other witnesses referred to existing local registers in the cities of Amsterdam and Helsinki[226] and to the list of technologies published by New Zealand Police[227] to demonstrate that establishing a register was not impractical, although we note that these registers appear to refer to city-run services such as libraries and parking.

108. The scope of the register was subject to debate among those who favoured one. When some circumscribed their recommendation to "the application of the law"[228] or "the criminal justice system"[229] only, others advised that it should cover "the public sector"[230] or "Government"[231] in general. The content of the register was also subject to a variety of opinions: beyond some basic information about what algorithms are being used, where, by whom, and since when, different witnesses were expecting different types of additions to the register.

- Professor Gavaghan recommended that "the purpose for which the technology is being used"[232] be clarified for each entry in the register.
- Big Brother Watch would expect public-private information-sharing agreements to be included.[233]

[218] Written evidence from the NCC Group (NTL0005)
[219] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)
[220] Written evidence from BAE Systems (NTL0056)
[221] Written evidence from the NCC Group (NTL0005). For an explanation, see paragraph 1.3.3.
[222] Q 78 (David Lewis)
[223] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035)
[224] Q 78 (Dr Liam Owens), written evidence from BAE Systems (NTL0056)
[225] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035). See also Q 78 (David Lewis).
[226] Written evidence from the Information Commissioner's Office (NTL0016)
[227] Written evidence from Professor Colin Gavaghan (NTL0047)
[228] Written evidence from Big Brother Watch (NTL0037)
[229] Q 11 (Professor Sylvie Delacroix)
[230] Q 65 (Professor Karen Yeung)
[231] Written evidence from the Public Law Project (NTL0046)
[232] Written evidence from Professor Colin Gavaghan (NTL0047)
[233] Written evidence from Big Brother Watch (NTL0037)

- The Public Law Project considered that each entry in the register should be accompanied with "executable versions of listed algorithms" and an explanation of how the technology works.[234]
- Citing the EU's proposed AI Regulation currently being discussed within the European Union as a reference (see Box 6), Professor Sandra Wachter suggested that the register could include algorithms themselves, the data on which they are trained, as well as information on tests carried out and on oversight mechanisms.[235]
- Several witnesses asked for "detailed impact assessments"[236] to be included, such as Equality Impact Assessments[237] or Human Rights Impact Assessments.[238]

The Algorithmic Transparency Standard

109. The Government has taken steps to publish some information to enhance transparency. The "Algorithmic Transparency Standard", launched in November 2021, has arisen from a recommendation by the Centre for Data Ethics and Innovation (CDEI) that "the UK Government should place a mandatory transparency obligation on public sector organisations using algorithms to support significant decisions affecting individuals".[239] The Standard includes basic information about what algorithmic tools are being used, how, and why, effectively constituting a non-exhaustive list. The Standard is a pilot and is due to conclude in 2022, when it will be reviewed and further developed. The Government states that:

> "By publishing this information proactively, the UK Government is empowering experts and the public to engage with the data and provide external scrutiny. Greater transparency will also promote trustworthy innovation by providing better visibility of the use of algorithms across the public sector, and enabling unintended consequences to be mitigated early on."[240]

110. While an extended version of the Standard has the potential to address the current lack of transparency, participation is voluntary and algorithms must meet strict eligibility criteria to feature in it. The information provided may also be partial. Participation would need to become mandatory, and the scope of the collection would need to be expanded, for it to become a satisfactory register of algorithms in the public sector.

111. For such a register to be reliable—that is; accurate, up to date, and complete—review of the entries would be needed, along with some form of penalty for failing to complete submissions satisfactorily. Responsibility for maintaining the register would also need to be assigned, alongside dedicated resources to

[234] Written evidence from the Public Law Project (NTL0046)

[235] Q 78 (Professor Sandra Wachter)

[236] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021)

[237] Q 65 (Silkie Carlo and Peter Dawson)

[238] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035)

[239] Cabinet Office, *UK government publishes pioneering standard for algorithmic transparency*: (29 November 2021): https://www.gov.uk/government/news/uk-government-publishes-pioneering-standard-for-algorithmic-transparency [accessed 11 January 2022].

[240] Cabinet Office, *UK government publishes pioneering standard for algorithmic transparency*

allow public bodies the time to submit entries without diverting effort away from operational activities.

112. ***Full participation in the Algorithmic Transparency Standard collection should become mandatory, and its scope extended to become inclusive of all advanced algorithms used in the application of the law that have direct or indirect implications for individuals. This would have the effect of turning the collection into a register. Engaging with this register will require additional and dedicated resourcing. The central body we have recommended should have the power to review and issue penalties if entries are not completed.***

113. ***The register should be user-friendly. Users should be able to find information about technological solutions being deployed, who is deploying them, where, on what occasions, and for what purposes. They should also be able to find detailed impact assessments and details of the certification issued by the central body we have recommended (see paragraph 189).***

CHAPTER 4: HUMAN-TECHNOLOGY INTERACTIONS

114. Our evidence showed that those who use technological solutions are not always engaging meaningfully with them. In this chapter, we discuss what ‘meaningful engagement’ means and why it may not always occur. The presence of an algorithm in these processes is not in itself cause for concern—a tool cannot, for example, arrest an individual, move a prisoner to a more secure prison, or make a legal judgment. Its presence can be insightful, enabling users to collate data, “link offences”[241], and join dots to better support communities and individuals. Advanced technologies are at their most useful when the human benefits from this insight: assessing it, considering it alongside other information, and not being bound by it. Key for us, as we began this inquiry, was how far advanced technologies inform or shape such important decisions, and whether the human is always the decision maker. Speaking to us in October 2021, the Home Secretary was very clear: “decisions about people will always be made by people.”[242] Our evidence paints a much more complicated—and problematic—picture.

Achieving interaction

115. Several of our witnesses stressed the importance of ensuring that there remains a “human in the loop”, meaning that a human should play a real (rather than nominal) role in any process involving technological solutions.[243] Silkie Carlo, Director of Big Brother Watch, told us that there should rather be “a machine in the loop of human decision-making”,[244] emphasising that human decision-makers should retain ownership and overall control of these processes. The Crown Prosecution Service was clear, for example, that “there are many skills that are uniquely human and always will be”.[245]

116. Witnesses did point out that humans themselves are biased, flawed, and often over-stretched. Silkie Carlo was concerned that focusing excessively on meaningful human engagement could cause a false sense of security, and cautioned against the neglect of other safeguards.[246] This was echoed by a group of facial recognition specialists, who wrote that “human intervention is necessary but not *sufficient* to ensure proper use”.[247]

117. The UK’s current data protection regime, the General Data Protection Act 2018, provides that a person “shall have the right not to be subject to a decision based *solely* on automated processing, including ‘profiling’, which produces legal effects concerning him or her or similarly significantly affects him or her.”[248] Part 3 of the Data Protection Act 2018 also requires that a law

[241] Written evidence from the Metropolitan Police Service (NTL0031)

[242] Oral evidence taken on 27 October 2021 (Session 2021–22), Q 13 (The Rt Hon Priti Patel MP, Home Secretary)

[243] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017), Public Law Project (NTL0046) and BAE Systems (NTL0056). Also see Q 46 (Professor Colin Gavaghan), Q 86 (Professor Paul Taylor), Q 86 (David Tucker), and Q 101 (Kit Malthouse MP)

[244] Q 58 (Silkie Carlo)

[245] Written evidence from the Crown Prosecution Service (NTL0018)

[246] Q 59 (Silkie Carlo)

[247] Written evidence from Dr David White *et al.* (NTL0012)

[248] Article 22 of Regulation (EU) 2016/679 of 23 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Article 22) 4 May 2016 (OJ L 119/1), see written evidence from Professor Nigel Harvey and Tobias Harvey (NTL0025) see also written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035)

enforcement body may not take a qualifying significant decision based *solely* on automated processing unless that decision is required or authorised by law.[249] These provisions aim to guarantee that there is a "human in the loop" but only for narrowly specified decisions. They do not prohibit decisions where automated processing has been a very significant, but not quite the sole, factor, and some exemptions apply.[250]

118. In reference to the Home Secretary's statement that "decisions about people will always be made by people"[251], National Policing Chief Scientific Adviser Professor Paul Taylor added a caveat. He told us that it "is almost entirely the case".[252]

Objective: meaningful interactions

119. Much of our evidence referred to the necessity of achieving "meaningful" human engagement with an automated tool, and its output.[253] Professor Michael Wooldridge, Head of the Computer Science Department at the University of Oxford, believed strongly that no technological tool, which he described as a "big long list of numbers", should "ever be more than another voice in the room".[254] A human can bring an understanding of ethics and context, and weigh outputs alongside other considerations which a technological tool cannot. There is an opportunity cost, for example, in prioritising one investigation over another.

120. The word 'meaningful' was explained by a European Commission Working Party for the purposes of the General Data Protection Regulation (GDPR):

> "To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data."[255]

121. The Information Commissioner's Office has issued non-binding guidance aimed to help organisations achieve "meaningful" human involvement. They have identified three key requirements:

- "human reviewers must be involved in checking the system's recommendation and should not just apply the automated recommendation to an individual in a routine fashion;
- reviewers' involvement must be active and not just a token gesture. They should have actual 'meaningful' influence on the decision, including the 'authority and competence' to go against the recommendation; and

[249] A 'qualifying significant decision' is defined as a decision which significantly affects or produces an adverse legal effect on an individual and is authorised by law. Data Protection Act 2018, section 49

[250] Written evidence from Big Brother Watch (NTL0037). For the relevant legislation see Data Protection Act 2018, section 14(4). Under the Data Protection Act 2018, some "qualifying significant decisions" can be made based solely on automated processing, but the data subject must be notified in writing.

[251] Oral evidence taken on 27 October 2021 (Session 2021–22) Q 13 (The Rt Hon Priti Patel MP, Home Secretary)

[252] Q 86 (Professor Paul Taylor)

[253] See, for example, written evidence from the Law Society of England and Wales (NTL0023), Big Brother Watch (NTL0037) and the Public Law Project (NTL0046)

[254] Q 33 (Professor Michael Wooldridge)

[255] European Commission, *Guidelines on Automated individual decision making and Profiling for the purposes of regulation 2016/679 (wp251rev.01)*, 22 August 2018: https://ec.europa.eu/newsroom/article29/redirection/document/49826 [accessed 24 January 2022]

- reviewers must 'weigh-up' and 'interpret' the recommendation, consider all available input data, and also take into account other additional factors."[256]

122. The importance of realising the principles of meaningful human engagement is widely recognised by Government Departments and public bodies. Evidence from the Ministry of Justice stated that "operational decisions are informed by analytical tools rather than being automatic consequences of tool outputs."[257] Similarly, the Home Office stated that they "strongly disagree … that we are allowing sensitive decisions to be delegated to machines in a way that is either contrary to the law or the core principles of the [criminal justice system]".[258]

Interactions to date

123. It was clear to us that current human-technology interactions are not consistently meaningful. We have learnt that, in many cases, the outputs of advanced technological tools can be accepted too readily, and that human involvement can be limited to clicking a button confirming the algorithmic suggestion. We were told about a human tendency to think of technologies as more objective and to "blindly trust [them]".[259] This was described by Professor Raab as a possible "culture of deference".[260] Professor Nigel Harvey and Mr Tobias Harvey thought that over time, operators and monitors "may become complacent and place too much trust in automated systems".[261] This could mean a human providing a very casual automatic sign off to the algorithmic suggestion, and embarking on the next logical step based on the prediction.

A lack of understanding

124. A pervasive lack of understanding of how algorithmic tools work may contribute to this tendency. A security consultancy, NCC Group, told us that even some developers "will deploy ML and AI systems without necessarily understanding their underlying mathematics and associated operations".[262] While understanding was said to be "developing"[263], we were given plenty of examples of where it was lacking. We were told, for instance, that attendees to an event about facial recognition (many of whom had access to and used facial recognition technology) "had a limited understanding of both face recognition technology and human face recognition."[264] A supplier of some tools had found that "criminal justice professionals are typically also lacking an expert, or even good, understanding."[265] Dee Masters and Robin Allen QC had, similarly, "become increasingly aware of the lack of understanding by regulators and the general public of the way in which AI systems are being used in their field of activity."[266]

[256] Information Commissioner's Office, 'Guidance on AI and data protection': https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-artificial-intelligence-and-data-protection/ [accessed 17 January 2022]
[257] Written evidence from the Ministry of Justice (NTL0053)
[258] Written evidence from the Home Office (NTL0055)
[259] Written evidence from BAE systems (NTL0056)
[260] Q 8 (Professor Charles Raab)
[261] Written evidence from Professor Nigel Harvey and Tobias Harvey (NTL0025)
[262] Written evidence from NCC Group (NTL0005)
[263] Written evidence from Archie Drake and Perry Keller (NTL0011)
[264] Written evidence from Dr Eilidh Noyes and Dr Reuben Moreton (NTL0026)
[265] Written evidence from SAS UK&I (NTL0041)
[266] Written evidence from Robin Allen QC and Dee Masters (NTL0019)

125. Clearly, a limited understanding is problematic in enabling meaningful engagement with an algorithmic output. Professor Carole McCartney, Professor of Law and Criminal Justice at the University of Northumbria, explained this further:

> "If the humans do not understand the technology and how it is working, how will they spot if it has failed or if they have made a mistake? … The humans have to understand how it is working in order to be able to spot the times when they need to not trust the technology".[267]

126. The Prison Reform Trust were similarly concerned about confidence to challenge outcomes which might appear discriminatory: "managers and policy makers are likely to be less inclined to 'look under the bonnet' when the technology they find there is unfamiliar."[268] The lack of understanding does not only apply to the people who are using the tool, but to those who commission it—and those who interact with its outputs later 'down the justice pipeline', including judiciary reviewing the conduct and findings of an investigation.

"A culture of deference"

127. In the absence of a "meaningful" interaction and of a sound understanding of a technological solution, a user may lack the time and confidence to challenge the output suggested by the programme. Algorithms, therefore, may become the *de facto* decision maker. Although written policies may state that humans retain overall decision-making prerogative, in practice the design of the algorithmic tool, the structure in which the algorithm is operating and the culture of the organisation may all serve to signal to the human that they should defer to the algorithmic output. On the whole, contributors referred to "risks" or "potential" of this tendency but did provide examples of processes subject to this risk. The examples below indicate particularly high stakes.

- The Durham Harm Assessment Risk Tool (HART) was a machine learning programme which used years of custody records and 34 pieces of individual data to predict whether someone could be classified as "medium risk" of reoffending. This classification assisted decision-making about eligibility for a rehabilitation programme. A group of contributors from the University of Essex were concerned that with this tool, "any potential tendency to defer or over-rely on automated outputs over other available information has the ability to transform what is still considered to be a human-led decision to *de facto* an automated one."[269] As outlined in paragraph 101, in September 2020, the HART tool was withdrawn. According to an article in policing publication *Police Professional*: "Hart's algorithm did noticeably better than its human counterparts". The article reported that while forecasts should not be used as an automated replacement for human judgement, they "can be used to support our officers, challenge them when they disagree with the algorithm, and steer us towards greater consistency and fairness".[270]

[267] Q 8 (Professor Carole McCartney)

[268] Written evidence from the Prison Reform Trust (NTL0004)

[269] Written evidence from Professor. Pete Fussey, Dr.Daragh Murray and Dr. Amy Stevens (NTL0017)

[270] Police Professional, *Artificial intelligence 'marginally better' at predicting re-offending* (25 January 2022): https://www.policeprofessional.com/news/artificial-intelligence-marginally-better-at-predicting-reoffending/ [accessed 24 February 2022]

- An automated triage system used by the Home Office, known as the sham marriage algorithm, is used to help "determine whether a proposed marriage should be investigated as a 'sham'". When a couple (of whom at least one is not a 'relevant national', or lacks appropriate immigration status or a valid visa) gives notice to be married, an algorithm sorts them into a 'red' or 'green' category. A red light is a flag for an investigation, and a human decision-maker then considers whether an investigation is needed. The Public Law Project told us that "The detail of the human review stage is unclear. We do not know whether the human decision maker exercises meaningful discretion."[271] An investigation can include interviews or home visits. If the couple does not comply with this investigation, they may not be allowed to marry. While the decision on the genuineness of the marriage is in the hands of an official, the Public Law Project were concerned that the human decision-maker may fall victim to "automation bias", defined as "a well-established psychological phenomenon whereby people put too much trust in computers".[272] The stakes are high: both marriage and immigration status may be at risk.

- Applications for clearance into the UK as part of border management are processed by Decision Making Centres, or 'hubs'. An algorithm to categorise these applications was referred to us by the Public Law Project as an "example of automation bias in action".[273] Applications are categorised by colour: red for high risk, amber for medium risk, and green for low risk. In 2016–17, an inspection of two hubs noted that with officials having only three minutes per decision and an assurance regime that "does not take account of the danger of 'automation bias', "there is a risk that the streaming tool becomes a *de facto* decision-making tool."[274] Following a legal case brought by campaigners, the tool has been removed from use.[275]

- Automated facial recognition provides possible "matches" between faces, which are "reviewed by trained officers before any intervention takes place".[276] Silkie Carlo thought that officers may be "assuming superiority from the machine's judgement" and making interventions without "applying genuinely their own analysis".[277] Research in operational settings had found that "any voice which confirmed the algorithm was upheld" and that "conversely, decisions not to intervene and stop an individual were often overturned."[278] Contributors were concerned about a tendency to defer to the match suggested by the tool:[279] in one independent report, only in eight of 42 matches had the technology been found to be correct.[280]

[271] Supplementary written evidence from the Public Law Project (NTL0059)

[272] Written evidence from the Public Law Project (NTL0046)

[273] Written evidence from Public Law Project (NTL0046)

[274] Independent Chief Inspector of Borders and Immigration, *An inspection of entry clearance processing operations in Croydon and Istanbul* (July 2017): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/631520/An-inspection-of-entry-clearance-processing-operations-in-Croydon-and-Istanbul1.pdf [accessed 17 January 2022]

[275] BBC, 'Home Office drops 'racist' algorithm from visa decisions' (4 August 2020): https://www.bbc.co.uk/news/technology-53650758 [accessed 2 February 2022]

[276] Written evidence from the Home Office (NTL0055)

[277] Q 58 (Silkie Carlo)

[278] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)

[279] See, for example, written evidence from Dr David White *et al.* (NTL0012).

[280] The Human Rights, Big Data and Technology Project, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (July 2019), p 10: http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf [accessed 7 February 2022]

128. **There is a significant and worrying body of evidence that the users of advanced technologies are in many cases failing to engage, in a meaningful way, with the output of automated processes. Outputs may be overrated or misinterpreted, and challenge smothered, with potentially significant adverse consequences for individuals and litigants.**

Explaining the over-reliance

129. Concerningly, we have been told that there was very little research to establish the reasons for a lack of meaningful engagement. Professor Karen Yeung told us that there is a lack of "robust, sustained and careful research to identify the conditions under which the use of these tools genuinely augments human decision making."[281]

130. ***The Home Office should, in conjunction with the Ministry of Justice and the College of Policing, undertake or commission appropriate research to determine how the use of predictive algorithms affects decision making, and under what circumstances meaningful human interaction is most likely.***

Empowering the human

131. Our witnesses shared their experience with us to indicate several ways human users can be empowered to engage meaningfully with technological solutions. Training, adequate guidance, and robust organisational mechanisms for dissent were raised.

Training

132. We were told that training would empower individual users to understand the outputs of algorithmic tools and ensure a level of confidence in challenging them. Professor Taylor told us that "most products come with a training package"[282] but it was indicated that this training was rarely mandatory or centralised, with David Tucker saying "there is very little mandatory training in policing."[283] The Public Law Project has said that it is "unclear" how much exists.[284] There are no legal requirements for users to be trained, nor any standards available for what available training should include. We were told, for example, that "There is currently no legal requirement for the operator of a facial recognition algorithm to possess any specific knowledge, skills, ability or expertise relevant to the role."[285]

133. David Lewis pointed out that training can help senior officers to be proactive and to act with "dynamism and confidence".[286] Peter Dawson, Director of the Prison Reform Trust, thought that training should go alongside an understanding of data interpretation, "understanding when a number is significant and when it is not", and confronting biases.[287] Training could also provide an understanding of the relevant equalities legislation and legal context more generally. Training, we were told, would need to be

[281] Q 58 (Professor Karen Yeung)

[282] Q 88 (Professor Paul Taylor). Given the practices of private companies we examine in Chapter 5, we cannot be confident that these training courses are robust, nor centred around a process of challenge.

[283] Q 87 (David Tucker)

[284] Written evidence from the Public Law Project (NTL0046)

[285] Written evidence from Dr Eilidh Noyes and Dr Reuben Moreton (NTL0026)

[286] Q 70 (David Lewis)

[287] Q 58 (Peter Dawson)

ongoing[288], and regularly reviewed.[289] It could also address a skills shortage in the workforce: references were made in the evidence to the difficulty in attracting employees highly skilled in technological tools who can command extremely high salaries in the private sector.[290]

134. Police bodies were cautious about instituting training before a tool has "settled down". David Tucker, Head of Criminal Justice at the College of Policing, told the Committee that "we have to wait for a moment of maturity, because if we do not we run the risk of trying to give guidance on something that has not settled down and is developing."[291] We are unconvinced by this argument. While tool-specific training is necessary, general training on the legislative context, the possibility of bias, and the need for cautious interpretation of outputs could be delivered to users before any particular tool is in use. David Tucker's view also appears to rest upon the assumption that most technologies are very new. While some are new, others (such as automated number plate recognition) have been in use for decades.[292]

135. We have seen material evidence of efforts and processes put in place to encourage meaningful human involvement. One significant step is the new office of the National Policing Chief Scientific Adviser. This post was established in May 2021 and the current postholder, Professor Paul Taylor, described his duties as including:

> "Ensuring that the decision-maker is always the officer, and talking about areas where sometimes that is not the case and how they might become over-reliant on technology, to give one example. There is also ensuring that we have systems and processes in place so that does not occur."[293]

The Ministry of Justice also outlined some of its safeguarding systems, which included "clear guidance" for "when the data should and should not be used, and support (and sometimes training) … made available to staff".[294]

136. While we acknowledge these provisions, there are no obligations for the consistent training of police officers or officials in the use of these systems, and the extent to which they should be relied on. It would not be reasonable to expect every police officer, or every Ministry of Justice official (to take but two examples), to be trained in data analytics and in the specificities of sophisticated technological solutions. Some will need to be trained, however, and they cannot be expected to undertake training of their own initiative. Training will need to be provided to them.

137. Solid understanding is essential for those who procure and deploy systems, and we address this in Chapter 5. Legal professionals and the judiciary may also sometimes need to interact with them in their work, for instance if they are concerned with criminal proceedings where algorithmic tools have played

[288] Written evidence from Professor Nigel Harvey and Tobias Harvey (NTL0025) and written evidence from Dr Eilidh Noyes and Dr Reuben Moreton (NTL0026)

[289] Written evidence from Dr David White *et al.* (NTL0012)

[290] Written evidence from the Serious Fraud Office (NTL0034)

[291] Q 91 (David Tucker)

[292] RUSI, 'Data analytics and algorithms in policing in England and Wales: Towards a new policy framework' (2020): https://rusi.org/explore-our-research/publications/occasional-papers/data-analytics-and-algorithms-policing-england-and-wales-towards-new-policy-framework [accessed 9 March 2022]

[293] Q 89 (Professor Paul Taylor)

[294] Written evidence from the Ministry of Justice (NTL0053)

a part,[295] and thus also need a thorough understanding of how algorithmic tools work. Tailored training for the relevant context, and delivered by the relevant professional body, will be required.

138. ***We endorse the principles provided by the Information Commissioner's Office regarding meaningful interaction with technologies. These principles should be applied through mandatory training for officers and officials using advanced technologies. As appropriate this should include both generic data analytics and specificities of the particular technology in question. As part of continuing professional development, training should also be made available to lawyers, members of the Judiciary, and other professionals involved in the justice system. Training will need to be tailored for the specific context and delivered by the relevant professional body with the support of the central body recommended in paragraph 44.***

139. ***At a minimum, there should be one person within every team which uses advanced technologies with the expertise required to support colleagues in the use of advanced technological solutions. Enabling meaningful support and proper assessment will require substantial investment in continuing professional development and the development of leadership skills.***

Guidance

140. In addition to training, the issuance of guidance could reinforce human-technological interactions. We have discussed this at length in Chapter 2 but will note here that guidance related to the use of specific technological solutions could and should include detailed information on challenging outputs of a specific tool.

Institutional facilitation

141. Along with training and guidance, we were alerted to several other necessary conditions for the challenge of algorithmic outputs. First, there must be sufficient staffing resource available. Simply put, people are required. On entry clearance processes (see paragraph 127), the Chief Inspector of Borders and Immigration had found that a dearth of staff had contributed to the tendency to rely overmuch upon the streaming tool.[296]

142. Second, appeal processes are needed. Professor Colin Gavaghan noted that signatories to the New Zealand algorithm charter commit to "providing a channel for challenging or appealing of decisions informed by algorithms."[297]

143. This need is recognised by Government Departments. The Ministry of Justice referred to their sexual offender predictive tool, which is supported by an "overarching" policy framework to "support consistency of use".[298] Evidence from the Prison Reform Trust acknowledged the need for structures and policies enabling a clear route for challenge, but emphasised that these must work well in practice.

[295] See paras 23–26

[296] Independent Chief Inspector of Borders and Immigration, *An inspection of entry clearance processing operations in Croydon and Istanbul*

[297] Written evidence from Professor Colin Gavaghan (NTL0047)

[298] Written evidence from the Ministry of Justice (NTL0053)

144. Peter Dawson, Director of the Prison Reform Trust, referred to an algorithm which helped to inform security categorisation for prisoners, the Digital Categorisation Service. Largely positive about the use of this tool, he nonetheless referred to some concerns about the policy frameworks in which it is used. He told us, for example, that the policy frameworks surrounding service were "shaky at best … there are good frameworks and they should work, but in practice they do not work well."[299] He also told us that, while the policy framework required a manager to ensure the system is functioning fairly, "there is no indication of how local managers are to be equipped to carry out such an analysis, or what changes they might be empowered to make once they have."[300]

145. Similarly, while assurance mechanisms were in place for the streaming tool examined by the Chief Inspector of Borders, he found that:

> "The assurance regime does not take account of the danger of 'confirmation bias' (an unconscious disinclination on the part of the decision maker to look for or give appropriate weight to evidence that contradicts the streaming rating, and tendency to select and rely on evidence that supports it)."[301]

146. ***Institutional processes to enable challenge to algorithmic outcomes should be reviewed and inspected. These inspections should also assess whether the users of the relevant tool(s) are appropriately trained.***

Improving the technology

147. Meaningful human-technology interactions can be achieved not only by empowering users, but also by improving technological solutions. Professor Delacroix told us "you can design these systems in a way that allows for interaction and even sometimes contestability, which is extremely important".[302] Our witnesses told us this would involve (re)designing interfaces and introducing "explainability" tools.

Designing interfaces

148. Human-technology interactions are affected by the design of technological interfaces—what the user sees when using a technological solution. A carefully designed interface can therefore improve human-technology interactions. Gary Pugh, the Forensic Science Regulator, told us that it was "critical that the requirements of regulation and other wider safeguards are built into the design of new technologies".[303]

149. We heard that some existing interfaces were imperfect. Professor Karen Yeung, for instance, warned against tools that produce "a nice colour" such as "a little risk assessment, red, green or yellow" because they are so "easy to interpret" that they do not encourage challenge or critical thinking.[304] In a similar vein, the Ministry of Justice told us that when designing "tools which

[299] Q 57 (Peter Dawson)
[300] Written evidence from the Prison Reform Trust (NTL0004)
[301] Independent Chief Inspector of Borders and Immigration, *An inspection of entry clearance processing operations in Croydon and Istanbul*
[302] Q 8 (Professor Delacroix)
[303] Written evidence from Gary Pugh (NTL0036)
[304] Q 57 (Professor Karen Yeung)

are used to support decisions about individuals", they "strive to ensure that the tool is designed to be intuitive."[305]

150. In response to the importance of interfaces and the temptation to simplify them excessively, the Bar Council told us that "safeguards should be incorporated as part of the design and creation of new technologies".[306] These could include information about how to interpret the algorithmic output, what information was used to reach it, an invitation to challenge the output, or a mention of applicable legal requirements. Because "transparency means different things to different users"[307], interfaces should be adaptable to different users. A front-line officer needing to make a quick decision will not require the same information as their manager reviewing a technological solution's overall performance (including if they wish to review efficiency claims made by sellers) or a legal professional reviewing its use in a criminal case.[308]

Explainability

151. We also heard that human-technology interactions could be improved if technological solutions were made more 'explainable'. We have dubbed this 'explainability', namely the ability to explain how a specific outcome was reached. The nature and depth of information provided would depend on who the outcome is being explained to—we heard that new technologies used for the application of the law should not only be explainable to those directly affected,[309] but also to end users and their managers,[310] judges and members of the legal profession,[311] and, as Professor Sylvie Delacroix, Professor in Law and Ethics at the University of Birmingham pointed out, to the general public.[312]

152. We were told that explainability was "crucial".[313] Professor Colin Gavaghan told us that "there is no perfect way of gaining access" to the reasons that motivated a decision by a human. If achieved, algorithmic explainability would therefore provide more compelling explanations of decisions than humans currently provide.[314] Certainly, procurement managers need to understand how the tools they are commissioning or purchasing function.[315] Importantly, Professor Wachter added that introducing an explainability requirement on technologies used for the application of the law could help with this:

> "When people do not want to tell you how [a technological solution] is working, it is either because they do not want to or because they do

[305] Written evidence from the Ministry of Justice (NTL0053)

[306] Written evidence from the Bar Council (NTL0048)

[307] Written evidence from BAE Systems (NTL0056)

[308] See Marion Oswald, 'Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power', *University of Winchester,* (6 August 2018), p 8–9: https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0359 [accessed 2 February 2022]

[309] Written evidence from Big Brother Watch (NTL0037)

[310] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)

[311] Written evidence from the Serious Fraud Office (NTL0034) and Archie Drake and Perry Keller (NTL0011)

[312] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035) and Q 11 (Professor Sylvie Delacroix)

[313] Written evidence from the Royal Statistical Society (NTL0033)

[314] Written evidence from Professor Colin Gavaghan (NTL0047)

[315] Chapter 5 addresses this from the angle of evaluations.

> not know. I do not think either is acceptable, especially in the criminal justice sector. If they claim that it is too complex, you might be better advised to use a system that is easier to understand".[316]

153. Nevertheless, we heard that new technologies used for the application of the law were rarely explainable.[317] The Metropolitan Police Service acknowledged that "some particularly complex algorithms may be known to have an effective output needed by policing but the process to get to that output can be hard to understand and explain."[318]

154. Witnesses told us about ways of achieving explainability. The Information Commissioner's Office flagged their published guidance on explainability, co-authored with the Alan Turing Institute.[319] Professor Sandra Wachter and Dr Brent Mittelstadt also told us about "counterfactual explanations" designed to provide individual explanations about an algorithmic outcome.[320]

Box 11: Counterfactual explanations

Professor Sandra Wachter and Dr Brent Mittelstadt told us about counterfactual explanations as a possible solution, among others, to increase explainability. Counterfactual explanations, they told us, consist in statements "that describe a small possible change to a case, or to the world, that would have led to a different outcome" in a specific case. One such statement could be: "You were denied parole because you had 4 prior arrests. If you had 2 prior arrests, you would have been granted parole."

If scaled up into a "bias test", they told us that these counterfactual explanations could be used as an "alarm system". Looking at an algorithm's behaviour in a series of cases, a bias test can produce a statement such as: "Your current decision system is not granting Black people parole at a comparable rate to other groups. Is this on purpose?"

According to our witnesses, this alarm could "allow judges and the police to investigate the decision criteria, design decisions, or unintended biases" embedded in a technological solution.[321] This tool has been released and is in use commercially.

155. ***There should be a requirement upon producers of technological products to embed explainability within the tools themselves. The interface of tools should be designed to facilitate the experience of users: equipping them with the necessary information to interpret outputs, and an indication of the level of surety its outputs provide. The specifics of what should be explained will vary depending upon the context. The tool should reflect that variation, and encourage users to consider and challenge results.***

[316] Q 80 (Professor Sandra Wachter)

[317] Written evidence from Professor Nigel Harvey and Tobias Harvey (NTL0025)

[318] Written evidence from the Metropolitan Police Service (NTL0031)

[319] Written evidence from the Information Commissioner's Office (NTL0016). Also see the Information Commissioner's Office, 'Explaining decisions made with AI': https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence/ [accessed 2 February 2022].

[320] Written evidence from Professor Sandra Wachter and Dr Brent Mittelstadt (NTL0058)

[321] *Ibid.*

CHAPTER 5: EVALUATION AND OVERSIGHT

156. A variety of mechanisms could address some of the common issues detailed in previous chapters. In this chapter, we discuss how systematic evaluations before a technology is deployed could support police forces and public bodies when procuring new technologies. Because new technologies need constant monitoring, we also discuss oversight mechanisms designed to ensure that technological solutions are continuingly evaluated throughout their lifecycle and in their specific deployment contexts. The evidence received has largely been in relation to police forces, but the conclusions of this chapter are valid for all public bodies involved in the application of the law.

Societal considerations

Biases

157. Our evidence referred repeatedly to the major issue of embedded biases: over 200 times in written evidence alone. We heard that it was present at every level of deployment: "Technologies are subject to bias in their development, use, and in the communication of technological capacities and their outcomes."[322] This bias can be unintentional and not easily visible. The Law Society of England and Wales told us that:

> "Bias, both conscious and unconscious, can be baked into algorithms and undermine consistently reliable results, and that using algorithms without questioning them or explaining them to the public could lead to decisions which threaten human rights and undermine trust in the justice system".[323]

158. This was most commonly explained by bias in the dataset used by the tool. Dr Leslie referred to "legacies of discrimination that have manifested in the type of large-scale datasets that have been needed to train" tools.[324] Giving specifics, Professor Karen Yeung pointed to "opinion data" used by the London Gangs Matrix, which "is based on opinions from police and other sources of intelligence". She said that the outcome of the Matrix's risk assessment was then "treated as if it is official objective evidence that this is a risky person".[325]

159. Much of our evidence referred to race. Professor Wachter referred to stop and search data (well recognised as a practice which impacts black people more than white people[326]) to argue that "explicit and implicit bias creeps in at various stages of the process … we cannot talk about ground truth so much." She said that "the only way to debias data is to debias humans."[327] There was general agreement that the use of advanced technologies could reproduce existing biases. Peter Dawson, Director of the Prison Reform Trust, for example, wrote that:

> "The unanswered question, therefore, is whether disproportionality is being driven by decisions and information from processes that precede

[322] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)

[323] Written evidence from the Law Society of England and Wales (NTL0023)

[324] Q 33 (Dr David Leslie)

[325] Q 57 (Professor Karen Yeung)

[326] HM Government, 'Ethnicity facts and figures: Stop and search' (February 2021): https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/stop-and-search/latest#byethnicity [accessed 7 February 2022]

[327] Q 71 (Professor Sandra Wachter)

> the application of the categorisation algorithm and on which it depends. Specifically, intelligence about BAME and Muslim men which cannot be effectively challenged, and which may reflect conscious or unconscious bias may be driving unfair treatment which the categorisation algorithm then cements".[328]

160. It was also clear that removing certain characteristics from a dataset would not solve the problem, as a number of other data points can act as "proxies".[329] Reference was even made to artificial datasets, with 'Mosaic' coming in for particular criticism—it groups people by profiling of characteristics. Big Brother Watch explained that the profiles:

> " … attribute 'demographic characteristics' to each stereotype. For example, 'Asian Heritage' individuals were characterised as being part of "extended families" living in "inexpensive, close-packed Victorian terraces", and that "when people do have jobs, they are generally in low paid routine occupations in transport or food service" … 'Families with Needs' were profiled as receiving "a range of benefits" with names like 'Stacey', while 'Low Income Workers' were typified as having "few qualifications" and were "heavy TV viewers" with names like 'Terrence' and 'Denise'."[330]

While we do not believe police forces are, at the present time, using Mosaic, there is no legal requirement preventing them from doing so.

161. Another frequent reference was to automated facial recognition.

- Professor Pete Fussey and his co-contributors told us that "differential performance across different ethnic, gender and age categories are established scientific facts."[331]
- Dr Kay Ritchie wrote, "Some algorithms gave rise to between 10 and 100 times more false positives for Asian and African American faces compared to Caucasian faces."[332]
- Professor Gavaghan told us about a facial recognition trial that was led by New Zealand Police. In this instance, "the algorithm simply was no use at recognising Māori or Pacific Island faces, probably because the dataset that it had been trained on did not contain many such faces."[333]
- When facial recognition technology was trialled by the Metropolitan Police Service, the force found that "there was a statistically significant issue with facial matching and sex."[334]

Impact assessments

162. Impact assessments can be a useful tool to identify and assess possible effects of the deployment of an algorithmic capability, including risks of discrimination resulting from biased technologies. Equality Impact

[328] Written evidence from the Prison Reform Trust (NTL0004)
[329] Written evidence from Liberty (NTL0020)
[330] Written evidence from Big Brother Watch (NTL0037)
[331] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)
[332] Written evidence from Dr Kay L Ritchie (NTL0003)
[333] Q 45 (Professor Colin Gavaghan)
[334] Q 53 (Silkie Carlo), see also Q 62 (Professor Karen Yeung) for a similar remark on the South Wales Police trial.

Assessments are a common approach to complying with the Public Sector Equality Duty,[335] while Data Protection Impact Assessments are required for data processing operations which are likely to result in a high risk to individuals.[336]

163. Various contributors argued for an extension of the current requirements, and evidence was very strongly in favour of requiring Equality Impact Assessments to be carried out in all cases where an algorithmic tool was deployed.[337] Police Scotland see Equality and Human Rights Impact Assessments as "crucial" to "ensure that emerging technologies are introduced in a proportionate and ethical manner".[338] They recommended they become mandatory. Others went further. Privacy International, for instance, argued that:

> "It is only acceptable to use new technologies for the application of the law if this is justified by an ex-ante assessment of the impact on fundamental rights (such as through Human Rights Impact Assessments ('HRIA') or Data Protection Impact Assessments ('DPIA')), with a strict assessment of the necessity and proportionality of using these technologies for their stated purpose."[339]

164. Some contributors argued for enhanced engagement with impact assessments. Professor Raab called for a broad approach to impact assessments, arguing that while they are "an appropriate place for addressing many questions", focusing requirements on data protection or privacy purposes "may miss crucial elements".[340] A review by the Centre for Data Ethics and Innovation appears to support this recommendation. It found that combining equality and data protection concerns into a combined Algorithmic Impact Assessment or Integrated Impact Assessment could "support a more consistent way of managing the regulatory and ethical risks raised by these technologies, including fairness."[341] It found also that, when only undertaken at the beginning of a process, risk assessments represent only one point in time and "should be seen as one tool complemented by others."[342]

165. Several witnesses recommended that "assessments should be published and consultation should be enabled in a real and transparent sense with both the public and civil society prior to deployment."[343] Prof Raab thought that publication could "be an important instrument in strengthening adherence to ethical principles, in gaining or retaining public confidence,

[335] House of Commons Library, *The Public Sector Equality Duty and Equality Impact Assessments*, Briefing Paper 06591, 8 July 2020

[336] Information Commissioner's Office, 'Data protection impact assessments': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments [accessed 21 January 2022]

[337] See, for example, written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021); Dr Matthias Wienroth *et al.* (NTL0022), Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035) and Privacy International (NTL0051)

[338] Written evidence from Police Scotland (NTL0043)

[339] Written evidence from Privacy International (NTL0051)

[340] Written evidence from Professor Charles Raab (NTL0014)

[341] Centre for Data Ethics and Innovation, *Review into bias in algorithmic decision making* (November 2020), p 126: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf [accessed 21 January 2022]

[342] *Ibid.*

[343] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035), see also written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkier and Professor Liz Campbell (NTL0021) and Q 65 (Silkie Carlo and Peter Dawson).

and in demonstrating trustworthiness in ways that are more convincing than slogans and pledges, or compliance with legal requirements.[344]

Community consultation

166. Dr Rosamunde van Brakel from Tilburg University told us that "evaluations need to be expanded to include impacts on society and communities" and that we should "get the affected communities involved in the policy decisions about implementing the technologies."[345] Professor Gavaghan concurred. He told us that representatives from communities should be involved "at an early stage" in the deployment and evaluation of technological solutions, so they can flag potential risks that technology providers and customers may have overlooked. Police Scotland thought that the use of emerging technologies posed challenges for "consultation and community engagement". They said that:

> "The way we engage the public and communities has a significant impact on the effectiveness of what we do to keep people safe and prevent crime. Being open and transparent about what we are doing and why is fundamental to maintain public confidence in policing."[346]

167. Others agreed that community consultation was important to ensure public trust and maintain the legitimacy of police forces.[347] It was felt that community engagement should focus on the potential uses of a new tool, with the Royal Statistical Society arguing that all law enforcement organisations using algorithms should "test the acceptability of the algorithm with affected groups".[348] We were told that consultation should be "open-ended and not instrumental" and that "it must allow for differences and tensions to be given a forum for articulation and negotiation."[349]

168. Police bodies noted the importance of community engagement and transparency, saying they were "an important part of the ethical use of technology."[350] The Metropolitan Police Service called for a code of practice to help inform community engagement but noted the difficulty in explaining particularly complex algorithms. This is, as we have noted in Chapter 4, a difficult problem to solve. If, however, the results of algorithmic processes are to be "understood and challenged by those affected"[351], this is a problem that must be solved. The impact assessment is the appropriate stage in the process.

169. ***Comprehensive impact assessments should be made mandatory for each occasion an advanced technological tool is implemented in a new context or for a new purpose. They should include considerations of bias; weaknesses of the specific technology and associated datasets; and discursive consideration of the wider societal and equality impacts (including explanations of public consultations). Impact assessments should be regularly updated and open to public scrutiny.***

[344] Written evidence from Professor Charles Raab (NTL0014)

[345] Q 46 (Dr Rosamunde van Brakel)

[346] Written evidence from Police Scotland (NTL0043)

[347] Written evidence from Dr Joe Purshouse, Dr Nessa Lynch, Dr Marcin Betkiern and Professor Liz Campbell (NTL0021)

[348] Written evidence from the Royal Statistical Society (NTL0033)

[349] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)

[350] Written evidence from the Metropolitan Police Service (NTL0031)

[351] Written evidence from Big Brother Watch (NTL0037)

Technical considerations

"The system will fail"

170. All technological solutions fail. Professor Wachter told us that "it is not a question of if but of when"[352], while Professor Wooldridge warned us that "technology is very brittle" and can fail in bizarre and unpredictable ways.[353] Failure may mean, for instance, that an AI solution designed to recognise faces would allocate the wrong name to the wrong person.[354] We were told that the deployment of a technological solution will normally depend on how often it fails. For instance, Policing Chief Scientific Adviser Professor Paul Taylor told us that, with solutions used for operational or investigative tasks, he "would have a very low tolerance for false positives". He noted though, that "there may be a different tolerance" for such failures in relation to "backstage" technological solutions.[355]

171. Sometimes, a technological solution will fail too often to be deployed at all. For instance, in 2020, the West Midlands Police (WMP) Ethics Committee was asked to consider the National Data Analytics Solution's Most Serious Violence model.[356] The Committee was concerned about the model's "accuracy rate" which, being below 50 per cent, is no better than tossing a coin. The Committee eventually unanimously recommended that the model did not proceed, and the consultative opinion of the Committee was followed.[357] The safeguard mechanism that the WMP Ethics Committee represents (see paragraphs 211–212) prevented deployment in this instance, enabling the project to focus on more promising models. In the absence of standards to which technologies must adhere, it is all too easy to imagine that it may have been deployed elsewhere—particularly in those areas which do not have the safeguard mechanisms of an ethics committee.

172. It is important not only to ask: "does it work?", crucial as that question is, but also: "does it work consistently?"; "is it safe?"; and "should it be used in this context at all?". David Leslie said there were "a few quasi-technical dimensions" that must be assessed to ascertain that a technological solution is "able to achieve [its] intended purpose." He listed these dimensions as including: "accuracy and performance, reliability, security and robustness."[358]

[352] Q 71 (Professor Sandra Wachter)
[353] Q 27 and Q 32 (Professor Michael Wooldridge)
[354] Q 27 (Professor Michael Wooldridge)
[355] Q 95 (Professor Paul Taylor), see also Q 96 (David Tucker).
[356] The Youth and Most Serious Violence aimed to consider whether there were particular factors that could inform why or when young people get involved in serious violence.
[357] Written evidence from Archie Drake and Perry Keller (NTL0011), see also West Midlands Police and Crime Commissioner Ethics Committee, 'EC Minutes and Advice' (1 July 2020): https://www.westmidlands-pcc.gov.uk/ethics-committee/ethics-committee-reports-and-minutes [accessed 25 February 2022].
[358] Q 27 (Dr David Leslie), see also written evidence from NCC Group (NTL0005).

Box 12: Scientific standards

In this report, a reference to 'scientific standards' is intended to mean a regime of quality standards and processes consistently applied to a person or body developing, maintaining or manufacturing a particular scientific product or technology, providing a scientific service, or incorporating a scientific method into their public service, combined with independent regulatory enforcement.

Such scientific standards would include requirements in respect of:

- Reliability: Is the same result consistently produced when the process is repeated? Has the method or technology been tested and independently peer reviewed?
- Accuracy and performance: Does the technology produce correct or accepted results? Are measures of accuracy included? Has unacceptable bias been eliminated? Is it robust?
- Context and Evaluation: How should the technology or method be operated in the context in which it will be used, and how should it be evaluated and monitored? What actions should be taken to avoid errors, in particular those that could result in detriment to individuals?
- Validity: Is the technology or method suitable and relevant for the facts, action, decision, question or issue under consideration within the relevant legal context? In what circumstances should the technology or method be used/not used? Is it proportional to the need it attempts to meet?

173. ***Minimum scientific standards should be set centrally by the new national body we have recommended in paragraph 44. They should then be transposed into regulations through secondary legislation.***

Scientific evaluations

174. A technological solution's performance could be assessed through scientific evaluations which apply standards. Strict applications of standards can ensure that decisions, actions, and policies are based on the best available evidence and practice, and that they are relevant in the particular context. This supports the better performance of public functions with reliable scientific practices and advice. If applied over a sector, standards can create consistency of quality and practice and thus work towards equality of treatment. Application of scientific standards can also minimise the risk of failures and associated impacts on society. Investigating and examining a tool can also bring any limitations into the open, warning those who are using it to help make potentially life-changing decisions.

175. We heard that evaluations should involve both laboratory and live trials. Lab trials could more accurately assess a technological solution's core performance. For instance, in the case of live facial recognition, a technological solution's propensity to miss a person on a watchlist (also known as a 'false negative') can be assessed during a lab trial. In a live trial, however, the assessor simply cannot know whether someone on a watchlist walked past a camera without being identified.[359] NCC Group stressed the importance of live trials in "the wider environment in which the technologies are deployed"[360], thereby accounting for "the likely behaviours of users"[361] and other "operational

[359] Q 53 (Professor Karen Yeung)

[360] Written evidence from NCC Group (NTL0005)

[361] *Ibid.*

issues".[362] For instance, we heard that "the accuracy of face recognition technology depends on … the environment in which the technology is deployed" because "in real settings, images may be of suboptimal quality or environmental conditions may be inhibitory to realising the full accuracy of face recognition technology."[363]

176. Moreover, we were told that the choice of variables used in the design of a technological solution should be carefully assessed. The choice of variables is a subjective one; it "is not science, it is an art", as Professor Karen Yeung put it. She added that "there is no right or wrong way of doing it".[364] This leaves the door open for personal preferences and "institutional bias" to enter technological solutions.[365] For instance, a computer scientist may want to include shoe size as a variable in an algorithm predicting recidivism if they see a statistically significant correlation between the two, whereas a lawyer would be concerned about the relevance of that variable.[366] Peter Dawson gave an example of what this can mean in practice, telling us that the definition of race within the Digital Categorisation Service did not take account of "the subdivisions within race". He explained that "it is different in prison if you are black, compared with being mixed race, having an Asian background or a Gypsy/Roma/Traveller background", adding that "that level of sophistication needs to be added".[367]

177. Finally, we were told that technological solutions should be tested against biases.[368] We heard that several tools, known as "fairness metrics", could be used to that effect.[369] Our witnesses told us about one of such tools, known as the "Conditional Demographic Disparity" tool, that produces counterfactual explanations (see Box 11 on counterfactual explanations).[370]

A lack of evaluations

178. For all these reasons, we heard that there was "appetite … for proper scrutiny and evaluation processes to be put in place."[371] However, we were told that technological solutions were rarely evaluated. Professor Karen Yeung told us that "robust, sustained and careful research" is often lacking. Dr van Brakel, Professor Raab, and Silkie Carlo, Director of Big Brother Watch, all concurred.[372] Our witnesses explained that this may be the result of scarce human and financial resources within police forces, as well as of dubious selling practices by technology providers.

179. The ability of police forces to act as an 'intelligent client' is limited by the lack of human and financial resources to carry out scientific evaluations. Academics told us that it was "all too rare that authorities decline to adopt technology because of quality concerns"[373], which police representatives

[362] Written evidence from Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens (NTL0017)
[363] Written evidence from Dr Eilidh Noyes and Dr Reuben Moreton (NTL0026)
[364] Q 57 (Professor Yeung)
[365] Q 92 (Alun Michael)
[366] See Marion Oswald, 'Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power' (6 August 2018), p 10: https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0359 [accessed 25 January 2022]
[367] Q 60 (Peter Dawson)
[368] See, for instance, written evidence from the Royal Statistical Society (NTL0033).
[369] Written evidence from Professor Sandra Wachter and Dr Brent Mittelstadt (NTL0058)
[370] *Ibid.*
[371] Q 40 (Professor Colin Gavaghan)
[372] Q 66 (Silkie Carlo), Q 46 (Dr Rosamunde van Brakel), and Q 4 (Professor Charles Raab)
[373] Written evidence from Archie Drake and Perry Keller, Kings College London (NTL0011)

confirmed. Police and Crime Commissioner Darryl Preston acknowledged that “policing has not always been the most intelligent customer.”[374] Dr Matthias Wienroth *et al.* felt that this made forces “vulnerable as ‘customers’” of technological solutions.[375] Policing Chief Scientific Adviser Professor Paul Taylor told us that evaluating technologies that could be deployed for the application of the law “requires a level of resource that we simply do not have”.[376] This echoes Professor Yeung’s statement that robust research was “hard, time-consuming and expensive”.[377]

180. Our witnesses emphasised a lack of expertise within police forces. The APCC, NPCC, and PDS thought that expertise and understanding was “limited but growing”.[378] The Metropolitan Police Service (Met) told us about the challenges of using new technologies, and that living up to these challenges was “a hard thing to do”, “even for the Met, which benefits from some great people with significant expertise”.[379] Former Deputy Chief Constable David Lewis agreed that there are “pockets of poor practices”[380] where senior level officers lack experience procuring advanced technology, while Kit Malthouse MP, Minister for Crime and Policing, recognised that “there is variable skill and ability” in new technologies across police forces.[381]

181. Other witnesses emphasised the role of budgetary constraints. Some academics told us that “attempts to do more with less in terms of resources may drive uptake rather than clear evidence that the new technology improves results”.[382] This phenomenon was described by Professor Yeung as a “tendency to go for the digital quick fix”.[383] This sense of “digital excitement” and “digital enchantment”[384] was felt even at ministerial level, as we were shown by the references of the Minister for Crime and Policing to an algorithm that would identify those likely to be murderous—a tool that does not exist.[385]

182. We were told, however, that such “digital enchantment” may turn into budgetary disenchantment. While we cannot verify the claim that tens of millions of pounds had been “spent poorly on solutions that are unfit for purpose or projects that have little value”,[386] it concerns us. Minister Kit Malthouse MP, for instance, mentioned “some pretty poor decision-making” by Greater Manchester Police in relation to the choice of their internal management software, which proved to be “a terrible problem and a headache for them”.[387] The Information Commissioner’s Office (ICO)

[374] Q 94 (Darryl Preston)
[375] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)
[376] Q 92 (Professor Paul Taylor)
[377] Q 58 (Professor Karen Yeung)
[378] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs’ Council and Police Digital Service (NTL0049)
[379] Written evidence from the Metropolitan Police Service (NTL0031)
[380] Q 75 (David Lewis)
[381] Q 106 (Kit Malthouse MP)
[382] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035), see also Q 42 (Professor Joh)
[383] Q 58 (Professor Karen Yeung)
[384] *Ibid.*
[385] Q 99 (Kit Malthouse MP)
[386] Q 70 (Dr Liam Owens)
[387] Q 106 (Kit Malthouse MP). For more information see Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services, *Greater Manchester Police Integrated Operational Policing System (iOPS): An inspection to review the force’s action plan to reduce backlogs arising from the implementation of a new computer system* (March 2020): https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/greater-manchester-police-integrated-operational-policing-system.pdf [accessed 7 February 2022].

was also critical of the Government's justification for the increased use of polygraph testing—a technological solution with controversial scientific grounds. The ICO noted that "there is barely any discussion about the necessity and proportionality of the polygraph."[388]

Box 13: Polygraph testing

'Polygraph' is the name used for the combination of physical measuring devices, questioning process, algorithmic calculations and human interpretation claimed to be able to give an indication of whether a person is giving a deceptive answer to a question. It is based on the theory that the psychological process of lying results in physiological changes (such as increased sweat or alterations in breathing) that can be measured, interpreted, and correlated to deceptiveness. There are considerable differences of opinion as to the validity of this theory.

In many legal jurisdictions, there are restrictions on the use of polygraph test evidence in court proceedings. In England and Wales, polygraph tests are currently in use to monitor sex offenders released on licence and manage compliance with their licence conditions. The remit of the polygraph test has been expanded to domestic abuse offenders under the Domestic Abuse Act 2021 and as a method of monitoring terrorism offenders and compliance with Terrorism Prevention and Investigation Measures under the Counter-Terrorism and Sentencing Act 2021.

183. **Pre-deployment scientific evaluations of technological solutions designed for use in the application of the law would empower public bodies and agencies to use better and more effective tools more safely.**

184. **Individual police forces are ill-equipped to carry out systematic evaluation of technological solutions: they have neither the resources nor the expertise. Tools are deployed when they have not been sufficiently evaluated; risking the use of tools that either cannot do the job, or that have unacceptable impacts on society.**

Centralised certification

185. It was suggested to us that technological solutions could be systematically evaluated at central level before they are deployed. This option could address the practical difficulties organisations face in carrying out such evaluations themselves, and provide some assurance that technologies are meeting minimum standards.

186. The call for pre-deployment certification comes strongly from technology providers themselves. David Spreadborough, a forensic analyst, told us that "a technology introduced in the judiciary system should be validated and approved by people technically competent on the matter."[389] BAE Systems agreed that a designated body could "develop a certificate of conformance (or 'Kitemark'/CE label) for approved AI applications".[390] NCC Group concurred that it is "essential that clear processes are established to vet technologies before they are deployed"[391], whereas Dr Liam Owens of technology provider Semantics21 told us about a "review" by "an intermediary".[392]

[388] Written evidence from the Information Commissioner's Office (NTL0016)
[389] Written evidence from David Spreadborough (NTL0015)
[390] Written evidence from BAE Systems (NTL0056)
[391] Written evidence from NCC Group (NTL0005)
[392] Q 78 (Dr Liam Owens)

Privacy International agreed with them and detailed mechanisms by which a technological solution should be "approved for use".[393]

187. Pre-deployment certification would not be without substantial precedent. Quite apart from the clear example of licensing drugs before deployment, there are examples of some technological tools being certified before deployment. The Ministry of Justice referred us to a peer-reviewed research study that evaluated the OASys Sexual reoffending Predictor (OSP) before this technological solution was approved by the Sexual Offending Management Board of Her Majesty's Prison and Probation Service.[394] Similarly, the Public Law Project drew our attention to the proposed AI Regulation in the European Union, which foresees central "certification indicating conformity to regulatory standards."[395]

188. In theory, the College of Policing is the most appropriate body to set standards and 'kitemark' technological solutions. In a "fundamental review" published in February 2022, the College of Policing emphasises its role in "setting standards" and in "support[ing] the police to make the most effective use of data to reduce crime and keep people safe". The College of Policing, however, also acknowledged that it "has not yet lived up to [its] potential or fully delivered on the expectations that officers, staff and the public have of policing's professional body."[396] In a response to the review on 10 February 2022, Her Majesty's Chief Inspector of Constabulary Sir Thomas Winsor WS wrote that "in many respects, the College has no standards".[397] We do not have confidence in the capacity of the College of Policing to set standards for the use of new technologies for the application of the law and to certify products against them.

189. ***The new national body recommended in Chapter 2 should systematically certify technological solutions following evaluation and prior to their deployment. No technological solution should be deployed until the central body has confirmed it meets the minimum standards. After a transition period, this requirement should retrospectively be applied to technological solutions already in use.***

Procurement

190. Centralised certification by a national body does not mean that individual police forces would not be free to procure the technological solutions of their choice, among those certified. Procurement would remain a critical stage.

Localism

191. Some witnesses recommended that technology should be procured centrally. Former Deputy Chief Constable David Lewis told us that "there probably should be more centralised procurement", alluding to the success of "regional procurement hubs" bringing police forces together.[398] BAE Systems agreed

[393] Written evidence from Privacy International (NTL0051)

[394] Written evidence from the Ministry of Justice (NTL0053)

[395] Written evidence from Public Law Project (NTL0046)

[396] College of Policing, *Fundamental review of the College of Policing*: https://assets.college.police.uk/s3fs-public/2022–02/Fundamental-review-of-the-College-of-Policing.pdf [accessed 24 February 2022]

[397] HMICFRS, *Inspectorate with College standards letter* (10 February 2022): https://www.justiceinspectorates.gov.uk/hmicfrs/publication-html/inspectorate-relationship-with-college-standards-letter/ [accessed 24 February 2022]

[398] Q 77 (David Lewis)

that they "would support some form of centralised AI procurement within policing and justice."[399]

192. Police and Crime Commissioners Alun Michael and Darryl Preston were against centralised, or regionalised, procurement. They told us that "principles are set down at a national level, but the application of those principles has to be very much at the local level."[400] While the Police Digital Service (PDS) does provide a centralised procurement function for certain national products, written evidence from the APCC, the NPCC and PDS was clear that, in the main, local procurement was their preferred model. They told us: "Because these tools address local needs, they vary in their form and focus. Indeed, this variation underpins policing's extensive success in innovation."[401] Each police force does indeed have their own local context and priorities: what works for one force will not necessarily work for another. We appreciate the importance of local policing.

A range of procurement strategies

193. Under our recommendations, individual police forces will retain ownership of their procurement choices, which could be through a variety of mechanisms. Public bodies involved in the application of the law procure new technologies in various ways. Some choose to purchase privately developed, off-the-shelf products. For instance, West Yorkshire Police purchased its Corvus Integrated Offender Management (IOM) Case software from a private company.[402] The system is fed with data stored in record management systems, some of which are commercial products themselves.[403]

194. Others may prefer to develop their own technological solutions in-house. The Ministry of Justice and HM Prison & Probation Service have developed several of them, such as:

- the Offender Group Reconviction Score (OGRS), a "predictor of proven reoffending within one and two years of noncustodial sentence or discharge from custody"[404]
- the Offender Assessment System (OASys), which "aims to assess the risk of harm offenders pose to others and how likely an offender is to reoffend"[405]
- the Digital Categorisation Service (DCS), an algorithm used to support decisions on security categorisations in prisons. The algorithm is a "mechanism for making, recording and justifying categorisation decisions"[406]

195. Other public bodies may opt to arrange partnerships with each other or with a third party, such as a private company or a university. For instance, the "Patrol-Wise" algorithm was developed jointly between West Yorkshire

[399] Written evidence from BAE Systems (NTL0056)

[400] Q 85 (Alun Michael), see also Q 85 (Darryl Preston).

[401] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049)

[402] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)

[403] *Ibid.*

[404] *Ibid.*

[405] Written evidence from Big Brother Watch (NTL0037)

[406] Written evidence from the Prison Reform Trust (NTL0004)

Police and the University College London.[407] The National Data Analytics Solution, a nationwide project sponsored by the Home Office and led by West Midlands Police in partnership with the National Crime Agency and Accenture, also falls in this category.[408] We were told that, in New Zealand, such partnerships were "by far the most common practice" when the government procures technological solutions.[409]

196. **While technological solutions should systematically be evaluated and 'kitemarked' centrally, different police forces need different technological solutions, according to their local needs. Procurement should remain the prerogative of individual forces, their choice being only constrained to those technological solutions certified by the central body.**

Dubious selling practices

197. Procurement is not the comfort zone of all police forces.[410] Former Deputy Chief Constable David Lewis told us that police forces "lack confidence about procurement [and] compliance with regulation."[411]

198. This discomfort may be exacerbated by dubious selling practices (see also paragraph 9). We heard about companies refusing to engage constructively with customers such as police forces on confidentiality grounds.[412] Professor Yeung was concerned that some technology providers may invoke Intellectual Property rights to make "empty promises" on the representativeness of training data, hiding it from its customers, external reviewers, and courts. The Metropolitan Police Service also told us about "vendors being reluctant to share enough information citing reasons of commercial confidentiality." Archie Drake and Perry Keller from King's College London summarised that "public authorities looking to implement [technological solutions] are often not entitled to know much about the systems they are using because of suppliers' 'aggressive' commercial confidentiality standards and associated practices".[413]

199. We were also told that "vendors are over-claiming system capabilities for commercial advantage"[414], which a public customer cannot assess in the absence of scientific evaluations. The NCC Group told us that "many claims made by [Machine Learning] product vendors, predominantly about products' effectiveness in detecting threats, are often unproven, or not verified by independent third parties."[415] Even when accuracy rates advertised by providers are grounded in proper evaluations, we heard that they are not necessarily reflective of the technological solution's actual performance once deployed.[416] Professor Charles Raab added that salespeople are "very persuasive" and may sometimes exaggerate claims to the disadvantage of police forces.[417] A developer, Dr Liam Owens, confirmed that "forensics

[407] Written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040)
[408] See written evidence from the Information Commissioner's Office (NTL0016).
[409] Q 45 (Professor Colin Gavaghan)
[410] See paragraph 9 on international examples of police procurement.
[411] Q 73 (David Lewis)
[412] See, for instance, written evidence from Big Brother Watch (NTL0037)
[413] Written evidence from Archie Drake and Perry Keller (NTL0011)
[414] *Ibid.*
[415] Written evidence from the NCC Group (NTL0005)
[416] Written evidence from Dr Eilidh Noyes and Dr Reuben Moreton (NTL0026)
[417] Q 24 (Professor Charles Raab)

has been overtaken by marketing" because of salespeople who "will take something they do not understand and shout a number that they do not understand" to make accuracy claims.[418]

200. Witnesses drew our attention to a range of other inappropriate selling practices that could put police forces in difficult situations. For instance, West Midlands Police (WMP) was offered a technological solution designed to tackle organised car crime by the companies TransteknlIQ Ltd and Bikal. The minutes of WMP Ethics Committee in November 2021 note, in addition to other points, that TransteknlIQ appeared to be a dormant company.[419] Alun Michael also told us about the risk for a police force associated with "being too close to a supplier".[420] David Lewis confirmed that he was "certainly aware of issues" where technology suppliers have taken advantage of a "personal relationship with an organisation".[421] Professor Raab added that "the collaborative relationship between law enforcement and the private sector is … growing, opaque, and insufficiently regulated".[422]

Procurement guidelines

201. To guide their procurement choices, public bodies can refer to the *Guidelines for AI procurement*, produced by the Government Office for AI and published in June 2020. These guidelines notably help public bodies navigate a confusing and fragmented regulatory framework (see Chapter 2). The aim appears to be to foster and stimulate the use of AI through public procurement. Under the heading "What is the aim of the guidelines?" the document states:

> "Public procurement can be an enabler for the adoption of AI and could be used to improve public service delivery. Government's purchasing power can drive this innovation and spur growth in AI technologies development in the UK."

The guidelines "provide[s] a set of guiding principles on how to buy AI technology, as well as insights on tackling challenges that may arise during procurement. These are the first of such guidelines, and they are not exhaustive".[423] They were developed in collaboration with the World Economic Forum, which published its own set of guidelines the same month.[424]

202. David Lewis, former Deputy Chief Constable of Dorset Police and National Police Chiefs' Council lead on ethics, assured us that these guidelines "are already being adhered to by many bodies in procurement in policing".[425] The Association of Police and Crime Commissioners, the National Police

[418] Q 76 (Dr Liam Owens), see also written evidence from the Metropolitan Police Service (NTL0031).

[419] West Midlands Police and Crime Commissioner Ethics Committee, 'Minutes of a meeting held on Wednesday 3rd November 10:00–14:00 hours': https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2022/01/2021-11-03-EC-Minutes-and-Advice.pdf?x41638 [accessed 1 February 2022]

[420] Q 94 (Alun Michael)

[421] Q 75 (David Lewis

[422] Written evidence from Professor Charles Raab (NTL0014)

[423] Office for Artificial Intelligence, 'Guidelines for AI procurement' (8 June 2020): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990469/Guidelines_for_AI_procurement.pdf [accessed 26 January 2022]

[424] World Economic Forum, *AI Procurement Guidelines* (11 June 2020): https://www.weforum.org/reports/ai-procurement-in-a-box/ai-government-procurement-guidelines [accessed 26 January 2022]

[425] Q 73 (David Lewis)

Chiefs' Council, and the Police Digital Service confirmed that they "inform contract implementation and management".[426]

203. We were told that these guidelines were of limited use. BAE Systems argued that the guidelines should be "more technical", more "supplier-focused", and more specific to "policing and the justice context".[427] Professor Wachter told us that these "vague" guidelines were "not good enough" because they were too soft to induce change in procurement practices.[428] Dr Liam Owens agreed that the guidelines are "very broad" and "non-specific" and would need to be better tailored to address the needs of technology providers in the context of the application of the law.[429] Furthermore, this document refers to 'guidance' as well as 'guidelines'. This is confusing. Guidance has a formal status and, therefore, more strength than guidelines. The terms cannot be used interchangeably, and there must be clarity as to the status of each document.

204. The Government's guidelines for AI procurement do not include specific considerations of two important principles: transparency and accountability. Similar AI procurement guidelines published by the World Economic Forum[430] pay much greater attention to these important matters.[431] Neither do the Government's guidelines pay much attention to evaluation—they only "underline the need for [the customer] to understand the supplier's AI approach", which could be seen as a focus on appearing an attractive customer. The guideline that follows recommends that teams "draft evaluation questions that give [them] information about the algorithms and models" and gives only very limited and high-level examples of what these evaluations would seek to ascertain.[432]

205. **Police forces lack proficiency when procuring new technologies. Existing official guidelines on the procurement of new technologies are focused on promoting uptake of AI. The Guidelines for AI Procurement are insufficient to ensure that public bodies take account of all relevant factors in procuring new technologies for the application of the law.**

206. ***While police forces should remain free to procure the technological solutions of their choice among those certified by the new national body, they need extra support to become proficient customers of new technologies. Pre-deployment certification could, in itself, reassure them about the quality of the products they are procuring. Enhanced procurement guidelines are also needed.***

Continuing oversight

207. Pre-deployment evaluations and certification would not be sufficient in themselves to guarantee the integrity and acceptability of new technologies

[426] Written evidence from the Association of Police and Crime Commissioners, the National Police Chiefs' Council (NPCC) and the Police Digital Service (PDS) (NTL0049)

[427] Written evidence from BAE Systems (NTL0056)

[428] Q 75 (Professor Sandra Wachter)

[429] Q 75 (Dr Liam Owens)

[430] World Economic Forum, *AI Procurement Guidelines*

[431] These guidelines are only two examples of the over 80 sets of guidelines and ethical frameworks emanating from various organisations across the world; see written evidence from Professor Charles Raab (NTL0014) and Algorithm Watch, 'AI Ethics Guidelines Global Inventory' (9 April 2019): https://algorithmwatch.org/en/ai-ethics-guidelines-global-inventory/ [accessed 26 January 2022].

[432] World Economic Forum, *AI Procurement Guidelines*

used in the application of the law. Continuing evaluation is also needed. Our witnesses told us that "not only is it essential that clear processes are established to vet technologies before they are deployed, but there must also be mechanisms in place to ensure that their performance is continuingly evaluated."[433]

208. Our contributors specifically stressed the importance of assessing the necessity and proportionality of each deployment of new technologies in light of local circumstances and on an ongoing basis. Liberty told us that "just as laws and policies engaging human rights must be adequately prescribed by law, necessary, and a proportionate way of achieving a legitimate aim, the design and implementation of technologies must be subject to similarly robust scrutiny."[434] The Metropolitan Police Service told us that proportionality was a central concern, telling us: "When policing uses technology, it does so to meet a defined policing purpose which must justify any privacy intrusions."[435] This is clearly a positive approach, but Dr Matthias Wienroth *et al.* thought that there was a need for proactive justification. They wrote that the onus was on the state to "justify measures as necessary and proportionate. This has often not been evidenced prior to, or even subsequent to implementation."[436]

Local ethics committees

209. Local ethics committees may be one way of ensuring continuing oversight and assessing necessity and proportionality. Policing Chief Scientific Adviser Professor Paul Taylor noted that a few police forces have established specialist ethics committees to consider the use of technology, in addition to the generalist ethics committees that all police forces have. Professor Taylor viewed all these committees as an opportunity to ensure that "the human is in the loop".[437] A group of legal academics concurred, telling us that "advisory boards with external, independent experts from technological or interdisciplinary backgrounds can be a helpful addition to the existing governance structure."[438] They are well placed to assess whether the use of a technological solution is necessary and proportionate given the specific context in which it will be deployed. Such assessments cannot be carried out in abstract terms because they require intimate knowledge of deployment circumstances.

210. By carrying out those functions, Police and Crime Commissioner for South Wales, Alun Michael, told us that ethics committees can complement the work of PCCs in their duties to conduct "an independent check" on the work of Chief Constables.[439] Former Deputy Chief Constable David Lewis added that ethics committees could add value by bringing expertise, independence, and a snapshot of public opinion in decision-making processes.[440]

[433] Written evidence from NCC Group (NTL0005)
[434] Written evidence from Liberty (NTL0020)
[435] Written evidence from the Metropolitan Police Service (NTL0031)
[436] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)
[437] Q 86 (Professor Paul Taylor)
[438] Written evidence from Professor Lilian Edwards, Professor Derek McAuley, Dr Lachlan Urquhart and Dr Jiahong Chen (NTL0035)
[439] Q 86 (Alun Michael)
[440] Q 69 (David Lewis), see also written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049).

The West Midlands Ethics Committee model

211. The West Midlands Ethics Committee (see Box 14), which our Specialist Adviser chairs, was frequently mentioned in the evidence we received, and has informed Government thinking.[441] Several witnesses told us that it "embodies much best practice."[442] Witnesses referred to several characteristics of the Committee as contributors to a successful oversight function. These included:

- A recruitment based on merit, [443]; with independent membership[444] with a range of expertise; [445]
- A commitment to publish meetings papers, minutes and conclusions;[446]
- The Committee's independence from the police force whose use of technology it is scrutinising; and[447]
- The Committee's remit to consider technological solutions throughout their lifecycle.[448]

[441] See, for instance, Q 2 (Professor Carole McCartney), Q 110 (Kit Malthouse MP), also written evidence from Archie Drake and Perry Keller (NTL0011), and defenddigitalme (NTL0044)

[442] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049), see also Q 11 (Professor McCartney), Q 48 (Dr Rosamunde van Brakel), and written evidence from BAE Systems (NTL0056)

[443] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049)

[444] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049) and BAE Systems (NTL0056)

[445] Q 11 (Professor McCartney), Q 48 (Dr Rosamunde van Brakel) and written evidence from BAE Systems (NTL0056)

[446] Q 11 (Professor McCartney), written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049), and BAE Systems (NTL0056)

[447] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049), Archie Drake and Perry Keller (NTL0011) and BAE Systems (NTL0056)

[448] Written evidence from Association of Police and Crime Commissioners, National Police Chiefs' Council and Police Digital Service (NTL0049) and BAE Systems (NTL0056)

Box 14: The West Midlands Police Ethics Committee

- The West Midlands Police and Crime Commissioner (PCC) and West Midlands Police (WMP) jointly established a specialist Ethics Committee in early 2019. The Committee has an advisory function only. It has no separate statutory or independent legal existence or formal regulatory function.
- The Committee's role is to advise the PCC and Chief Constable (CC) on data science projects being developed by WMP's internal Data Analytics Lab, and on national policing data science projects in which WMP has an interest, such as the National Data Analytics Solution (NDAS). Its advice must be "pragmatic" and "appropriate for meaningfully advising the CC and PCC on how to move forward."[449]
- The Committee considers technological solutions throughout their lifecycle—from initial project proposal, to testing and proposed implementation. Its advice is grounded in the operational context in which technological solutions are used.
- The Committee's terms of reference contain a commitment to transparency. The Committee publishes papers and minutes, subject to any necessary operational confidentiality.
- The Chair, Vice-Chair, and Committee members are all independent volunteers recruited following an open application process.

212. The West Midlands Ethics Committee is relevant because it has a specific focus on ethical issues arising from technological solutions, and because it has inspired thinking on a national model.

A national ethics committee

213. On 3 November 2021, Baroness Williams of Trafford, Minister of State for the Home Office, told the House of Lords that the WMP Ethics Committee would inspire a national governance model for the use of data analytics in policing:

> "Work is also under way to develop a national data ethics governance model, building on the work West Midlands Police has done to establish an ethics committee to advise on data science projects. The national model will also be developed in collaboration with the Centre for Data Ethics and Innovation and the Home Office."[450]

This was later confirmed in the written evidence submitted by the Home Office.[451]

214. In evidence to us, however, Kit Malthouse MP made a rather different statement. He told us that he thought it was "a good idea for local police forces to have ethics committees" but that he viewed Parliament as the national ethics committee, that decides on "the legal and the moral framework within

[449] West Midlands Police Ethics Committee, 'Terms of Reference', para 47: https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2019/07/Ethics-Committee-Terms-of-Reference-as-at-1-April-2019.pdf?x41638 [accessed 1 February 2022]

[450] HL Deb, 3 November 2021, cols 1301–1305

[451] Written evidence from the Home Office (NTL0055)

which everything in society operates". Therefore, the Minister told us, he "would be concerned about setting up a parallel ethics group".[452]

215. Some witnesses had reservations about scaling up the WMP model. Professor Yeung, for instance, told us that she was "really worried" that the committee's views may be "disregarded" in the absence of any legal foundation for the committee itself.[453] We were also told that a lack of funding could make ethics committees vulnerable if they operate without a separately funded dedicated secretariat and are reliant on the dedication of its volunteer members.[454] This also raises the question of the social representativeness of the membership. Dr Matthias Wienroth *et al.* thought the experience of the WMP Ethics Committee "should be studied to understand their integrated role and oversight capacity, as well as their limitations".[455] Academics from the University of Northumbria also stressed the importance of a clear statutory basis, budget, and power for ethics committees to have the "capacity to scrutinise and hold technology developers, users and commissioners to account."[456]

216. **Oversight mechanisms are required to complement pre-deployment scientific evaluations of new technologies used for the application of the law. Local specialist ethics committees are best placed to scrutinise technological solutions throughout their lifecycle and in their deployment contexts.**

217. ***We urge the Government to continue work on the national data ethics governance body. This body will need the independence, resources, and statutory underpinning to enable it to scrutinise the deployment of new technologies and act as a central resource of best practice.***

218. ***The Home Office should encourage and facilitate the development of local or regional specialist ethics committees. These committees should be granted independence, a statutory basis, and an independent budget. They should be transparent, and their membership should be diverse. They should scrutinise the use of new technologies by police forces throughout their lifecycle and in their deployment contexts, confirming that their proposed and actual uses are legitimate, necessary, and proportionate. These committees could be given a veto of the deployment of a particular technological solution during a mandatory trial period.***

219. ***The new national body recommended in paragraph 44 would have distinct responsibilities to set minimum standards for the use of new technologies in the application of the law; certify every new technological solution against these standards; and to carry out regular audits into their use. With the assurance brought by the certification process and the register of algorithms, police forces and other public bodies would remain free to procure the technological solutions of their choice, as long as the products have been certified.***

[452] Q 107 (Kit Malthouse MP)

[453] Q 65 (Professor Karen Yeung)

[454] See written evidence from Dr Miri Zilka, Detective Sergeant Laurence Cartwright and Dr Adrian Weller (NTL0040).

[455] Written evidence from Dr Matthias Wienroth *et al.* (NTL0022)

[456] *Ibid.*

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

Legal and institutional frameworks

1. We see serious risks that an individual's right to a fair trial could be undermined by algorithmically manipulated evidence. We therefore favour precise documentation, evaluation by subject experts, and transparency where evidence may be subject to algorithmic manipulation. (Paragraph 26)

2. The use of advanced technologies in the application of the law poses a real and current risk to human rights and to the rule of law. Unless this is acknowledged and addressed, the potential benefits of using advanced technologies may be outweighed by the harm that will occur and the distrust it will create. (Paragraph 30)

3. We have heard no evidence that the Government has taken a cross-departmental strategic approach to the use of new technologies in the application of the law. There appears in practical terms to be a considerable disconnect across Government, exemplified by confusing and duplicative institutional oversight arrangements and resulting in a lack of coordination. Recent attempts to harmonise have instead further complicated an already crowded institutional landscape. Thorough review across Departments is urgently required. (Paragraph 41)

4. *We recommend that the Government rationalise the respective roles of Departments as they pertain to the use of new technologies in the application of the law.* (Paragraph 42)

5. *We recommend that the Government conduct a review to rationalise and consolidate governance structures of the use of technologies in the application of the law.* (Paragraph 43)

6. *As part of rationalisation, the Government should establish a single national body to govern the use of new technologies for the application of the law. The new national body should be independent, established on a statutory basis, and have its own budget. The body would have several functions and responsibilities, which we detail in Chapter 5. It should draw on as wide as possible a range of expertise.* (Paragraph 44)

7. While they play an essential role in addressing breaches of the law, we cannot expect the Courts to set the framework for the deployment of new technologies. (Paragraph 50)

8. Given the potential costs of technologies and the problems that can and do arise from their implementation, including with respect to privacy rights, freedoms, and discrimination, we consider that a stronger legal framework is required to prevent damage to the rule of law. (Paragraph 61)

9. *We recommend that the Government bring forward primary legislation which embodies general principles, and which is supported by detailed regulations setting minimum standards. We consider that this approach would strike the right balance between concerns that an overly prescriptive law could stifle innovation and the need to ensure safe and ethical use of technologies.* (Paragraph 65)

10. *Along with 41 other countries, the Government has endorsed principles of Artificial Intelligence. In response to this report, the Government should outline proposals to establish these firmly in statute.* (Paragraph 66)

11. *Guidance, both general and specific, is urgently needed. The Government should require that national guidance for the use of advanced technological tools in policing and criminal justice is drawn up and, as part of their response to this report, should outline concrete plans for this.* (Paragraph 74)

12. *There is a need for a 'one-stop shop' collating all relevant legislation, regulation and guidance and drawing together high-level principles with practical user guides. This collation should be updated by the College of Policing on an ongoing basis, and direct users to the guidance and regulation relevant to their circumstance and need.* (Paragraph 75)

13. There is no clear line of accountability for the misuse or failure of technological solutions used in the application of the law. As a result, no satisfactory recourse mechanisms exist. (Paragraph 84)

14. *The Government should appoint a taskforce to produce guidance to ensure that lines of accountability, which may differ depending on circumstances, are consistent across England and Wales. The taskforce should act transparently and consult with all affected parties.* (Paragraph 85)

15. *Moratoria are important and powerful mechanisms. In its response to this report, the Government should set out the circumstances in which it would be willing to deploy them in the future. The new national body we recommend should be empowered to refuse certification for a new tool under those circumstances.* (Paragraph 89)

Transparency

16. *One of the principles in the new statute we recommend should be transparency.* (Paragraph 94)

17. There are no systematic obligations on individual departments, public bodies, and police forces to disclose information on their use of advanced technological solutions. It is impossible for Parliament, press, academia, those responsible for procurement and—importantly—those subject to their use to scrutinise and challenge the use of technological solutions as they cannot know who is using what, for how long, for what purpose, or with what safeguards. This risks undermining trust in the police, the justice system, and the rule of law. (Paragraph 98)

18. *We urge the Government to consider what level of candour would be appropriate to require of police forces regarding their use of advanced technologies.* (Paragraph 102)

19. *Full participation in the Algorithmic Transparency Standard collection should become mandatory, and its scope extended to become inclusive of all advanced algorithms used in the application of the law that have direct or indirect implications for individuals. This would have the effect of turning the collection into a register. Engaging with this register will require additional and dedicated resourcing. The central body we have recommended should have the power to review and issue penalties if entries are not completed.* (Paragraph 112)

20. *The register should be user-friendly. Users should be able to find information about technological solutions being deployed, who is deploying them, where, on what occasions, and for what purposes. They should also be able to find detailed impact assessments and details of the certification issued by the central body we have recommended (see paragraph 189).* (Paragraph 113)

Human-technology interactions

21. There is a significant and worrying body of evidence that the users of advanced technologies are in many cases failing to engage, in a meaningful way, with the output of automated processes. Outputs may be overrated or misinterpreted, and challenge smothered, with potentially significant adverse consequences for individuals and litigants. (Paragraph 128)

22. *The Home Office should, in conjunction with the Ministry of Justice and the College of Policing, undertake or commission appropriate research to determine how the use of predictive algorithms affects decision making, and under what circumstances meaningful human interaction is most likely.* (Paragraph 130)

23. *We endorse the principles provided by the Information Commissioner's Office regarding meaningful interaction with technologies. These principles should be applied through mandatory training for officers and officials using advanced technologies. As appropriate this should include both generic data analytics and specificities of the particular technology in question. As part of continuing professional development, training should also be made available to lawyers, members of the Judiciary, and other professionals involved in the justice system. Training will need to be tailored for the specific context and delivered by the relevant professional body with the support of the central body recommended in paragraph 44.* (Paragraph 138)

24. *At a minimum, there should be one person within every team which uses advanced technologies with the expertise required to support colleagues in the use of advanced technological solutions. Enabling meaningful support and proper assessment will require substantial investment in continuing professional development and the development of leadership skills.* (Paragraph 139)

25. *Institutional processes to enable challenge to algorithmic outcomes should be reviewed and inspected. These inspections should also assess whether the users of the relevant tool(s) are appropriately trained.* (Paragraph 146)

26. *There should be a requirement upon producers of technological products to embed explainability within the tools themselves. The interface of tools should be designed to facilitate the experience of users: equipping them with the necessary information to interpret outputs, and an indication of the level of surety its outputs provide. The specifics of what should be explained will vary depending upon the context. The tool should reflect that variation, and encourage users to consider and challenge results.* (Paragraph 155)

Evaluation and oversight

27. *Comprehensive impact assessments should be made mandatory for each occasion an advanced technological tool is implemented in a new context or for a new purpose. They should include considerations of bias; weaknesses of the specific technology and associated datasets; and discursive consideration of the wider societal and equality impacts (including explanations of public consultations). Impact assessments should be regularly updated and open to public scrutiny.* (Paragraph 169)

28. *Minimum scientific standards should be set centrally by the new national body we have recommended in paragraph 44. They should then be transposed into regulations through secondary legislation.* (Paragraph 173)

29. Pre-deployment scientific evaluations of technological solutions designed for use in the application of the law would empower public bodies and agencies to use better and more effective tools more safely. (Paragraph 183)

30. Individual police forces are ill-equipped to carry out systematic evaluation of technological solutions: they have neither the resources nor the expertise. Tools are deployed when they have not been sufficiently evaluated; risking the use of tools that either cannot do the job, or that have unacceptable impacts on society. (Paragraph 184)

31. *The new national body recommended in Chapter 2 should systematically certify technological solutions following evaluation and prior to their deployment. No technological solution should be deployed until the central body has confirmed it meets the minimum standards. After a transition period, this requirement should retrospectively be applied to technological solutions already in use.* (Paragraph 189)

32. While technological solutions should systematically be evaluated and 'kitemarked' centrally, different police forces need different technological solutions, according to their local needs. Procurement should remain the prerogative of individual forces, their choice being only constrained to those technological solutions certified by the central body. (Paragraph 196)

33. Police forces lack proficiency when procuring new technologies. Existing official guidelines on the procurement of new technologies are focused on promoting uptake of AI. The Guidelines for AI Procurement are insufficient to ensure that public bodies take account of all relevant factors in procuring new technologies for the application of the law. (Paragraph 205)

34. *While police forces should remain free to procure the technological solutions of their choice among those certified by the new national body, they need extra support to become proficient customers of new technologies. Pre-deployment certification could, in itself, reassure them about the quality of the products they are procuring. Enhanced procurement guidelines are also needed.* (Paragraph 206)

35. Oversight mechanisms are required to complement pre-deployment scientific evaluations of new technologies used for the application of the law. Local specialist ethics committees are best placed to scrutinise technological solutions throughout their lifecycle and in their deployment contexts. (Paragraph 216)

36. *We urge the Government to continue work on the national data ethics governance body. This body will need the independence, resources, and statutory underpinning to enable it to scrutinise the deployment of new technologies and act as a central resource of best practice.* (Paragraph 217)

37. *The Home Office should encourage and facilitate the development of local or regional specialist ethics committees. These committees should be granted independence, a statutory basis, and an independent budget. They should be transparent, and their membership should be diverse. They should scrutinise the use of new technologies by police forces throughout their lifecycle and in their deployment contexts, confirming that their proposed and actual uses are legitimate, necessary, and proportionate. These committees could be given a veto of the deployment of a particular technological solution during a mandatory trial period.* (Paragraph 218)

38. *The new national body recommended in paragraph 44 would have distinct responsibilities to set minimum standards for the use of new technologies in the application of the law; certify every new technological solution against these standards; and to carry out regular audits into their use. With the assurance brought by the certification process and the register of algorithms, police forces and other*

public bodies would remain free to procure the technological solutions of their choice, as long as the products have been certified. (Paragraph 219)

APPENDIX 1: LIST OF MEMBERS AND DECLARATIONS OF INTEREST

Members

Lord Blunkett
Baroness Chakrabarti
Lord Dholakia
Baroness Hallett
Baroness Hamwee (Chair)
Lord Hunt of Wirral
Baroness Kennedy of The Shaws
Baroness Pidding
Baroness Primarolo
Lord Ricketts
Baroness Sanderson of Welton
Baroness of Shackleton of Belgravia

Declarations of Interest

Lord Blunkett

Non- Financial: Non-executive Chairman, Cyber Essentials Direct Limited

Directorship: Director and Chairman of the Board, University of Law Limited (subsidiary and affiliated institution of Global University Systems and Interactive Pro Limited)

Baroness Chakrabarti

No relevant interests to declare

Lord Dholakia

Trustee of the Police Foundation which produced a report on the Strategic Review of Policing in England and Wales on 8 March 2022

Baroness Hallett

Retired judge

Baroness Hamwee

No relevant interests to declare

Lord Hunt of Wirral

Partner, DAC Beachcroft LLP (International commercial law firm)

Honorary Bencher, Inner Temple

Baroness Kennedy of The Shaws

Member of Microsoft Technology and Human Rights Advisory Council

Baroness Pidding

No relevant interests to declare

Baroness Primarolo

Non-Executive Director on the Board of Thompson's Solicitors LLP.

Lord Ricketts

No relevant interests to declare

Baroness Sanderson of Welton

No relevant interests to declare

Baroness Shackleton of Belgravia

No relevant interests to declare other than those on the Register

Specialist Adviser

Dr Marion Oswald

Associate Professor, Northumbria Law School

Advisory Board member, Centre for Data Ethics and Innovation

Senior Research Associate, The Alan Turing Institute

Associate Fellow, Royal United Services Institute for Defence and Security Studies;

Independent Chair, West Midlands Police & Crime Commissioner and West Midlands Police Data Ethics Committee;

Member, New Zealand Police Expert Panel on Emergent Technologies;

Advisory board member of the UKRI Trustworthy Autonomous Systems Hub;

Member of the Royal Society Working Group on Privacy Enhancing Technologies (2018–19 and reconstituted 2021);

Member of National Statistician's Data Ethics Advisory Committee since its foundation (2016-date);

Executive member, British & Irish Law, Education & Technology Association;

Member, Arts and Humanities Research Council Peer Review College.

APPENDIX 2: LIST OF WITNESSES

Evidence is published online at https://committees.parliament.uk/committee/519/justice-and-home-affairs-committee/publications/ and available for inspection at the Parliamentary Archives (020 7219 3074).

Evidence received by the Committee is listed below in chronological order of oral evidence session and in alphabetical order. Those witnesses marked ** gave both oral evidence and written evidence. Those marked with * gave oral evidence and did not submit any written evidence. All other witnesses submitted written evidence only.

Oral evidence in chronological order

*	Professor Sylvie Delacroix, Professor in Law and Ethics at University of Birmingham	QQ 1–24
*	Professor Carole McCartney, Professor of Law and Criminal Justice at Northumbria University	QQ 1–24
**	Professor Charles Raab, Professorial Fellow, Politics and International Relations, School of Social and Political Science at The University of Edinburgh)	QQ 1–24
*	Dr David Leslie, Ethics Theme Lead at Alan Turing Institute	QQ 25–38
*	Professor Michael Wooldridge, Head of Department of Computer Science, Professor of Computer Science at University of Oxford	QQ 25–38
**	Professor Colin Gavaghan, Director New Zealand Law Foundation Centre for Law and Policy in Emerging Technologies at University of Otago	QQ 39–51
*	Professor Elizabeth E Joh, Martin Luther King Jr. Professor of Law at University of California, Davis	QQ 39–51
*	Dr Rosamunde Elise van Brakel, Co-Director, Surveillance Studies Network, Associate Professor Tilburg University/Vrije Universiteit Brussel (VUB)	QQ 39–51
**	Silkie Carlo, Director, Big Brother Watch	QQ 52–67
**	Peter Dawson, Director, Prison Reform Trust	QQ 52–67
*	Professor Karen Yeung, Interdisciplinary Professorial Fellow in Law, Ethics and Informatics, Birmingham Law School at The University of Birmingham	QQ 52–67
*	David Lewis, Former Deputy Chief Constable and former ethics lead NPCC at Dorset Police	QQ 68–82
*	Dr Liam Owens, Founder and Chief Executive Officer, Semantics 21	QQ 68–82
**	Professor Sandra Wachter, Associate Professor and Senior Research Fellow at University of Oxford	QQ 68–82
**	Professor Paul Taylor, Chief Scientific Adviser, National Police Chiefs' Council	QQ 83–98

★★	Alun Michael, Police and Crime Commissioner for South Wales and Joint Lead for Data and Bioethics, Association of Police and Crime Commissioners	QQ 83–98
★★	Darryl Preston, Police and Crime Commissioner for Cambridgeshire and Peterborough and Joint Lead for Data and Bioethics, Association of Police and Crime Commissioners	QQ 83–98
★	David Tucker, Faculty Lead on Crime and Criminal Justice, College of Policing.	QQ 83–98
★	The Rt Hon Kit Malthouse MP, Minister of State for Crime and Policing at the Home Office and Ministry of Justice	QQ 99–111
★	Dr Christophe Prince, Director for Data and Identity, Home Office	QQ 99–111

Alphabetical list of all witnesses

Robin Allen QC, Barristers at A1 Law Consultancy/ Cloisters Chambers	NTL0019
Dr Arianna Andreangeli, Senior Lecturer in Competition Law, Edinburgh Law School, University of Edinburgh	NTL0038 NTL0039
Dr Philip Avenell, Managing Director and Forensic Biologist at Forensic Access	NTL0024
Avon and Somerset Police	NTL0052
BAE Systems	NTL0056
Professor Melanie Bailey, Professor at University of Surrey	NTL0024
The Bar Council	NTL0048
Dr Marcin Betkier, Lecturer in Law at Victoria University of Wellington	NTL0021
Dr Stephen Bleay, Senior Lecturer in Forensic Science at London South Bank University	NTL0024
Katy Bourne OBE, Sussex Police and Crime Commissioner	NTL0045
Dr Rebecca Brown, Research Fellow at University of Oxford	NTL0030
Professor Dame Vicki Bruce DBE, Professor Emerita at Newcastle University	NTL0012
Professor A Mike Burton, Professor of Psychology at University of York	NTL0012
Professor Liz Campbell, Professor and Francine V McNiff Chair in Criminal Jurisprudence at Monash University	NTL0021

**	Silkie Carlo, Director, Big Brother Watch (QQ 52–67)	NTL0037
	Detective Sergeant Laurence Cartwright, Data Analytics lead at Sussex Police	NTL0040
	Dr Jiahong Chen, Lecturer in Law at Sheffield Law School, University of Sheffield	NTL0035
	The Crown Prosecution Service	NTL0018
	Dr Benjamin Davies, Wellcome Trust Society & Ethics Research Fellow at University of Oxford	NTL0030
**	Peter Dawson, Director, The Prison Reform Trust (QQ 52–67)	NTL0004
	defenddigitalme	NTL0044
	Dr Delphine Defossez (Lecturer in Law), Northumbria University	NTL0022
*	Professor Sylvie Delacroix, Professor in Law and Ethics at University of Birmingham (QQ 1–24)	
	Professor Thomas Douglas, Professor of Applied Philosophy University of Oxford	NTL0013 NTL0030
	Archie Drake, Research Associate at Kings College, London	NTL0011
	Professor Gary Edmond, Professor of Law at UNSW Sydney	NTL0012
	Professor Lilian Edwards, Professor of Law, Innovation and Society at Newcastle Law School, Newcastle University	NTL0035
	Professor Seena Fazel, Professor of Forensic Psychiatry & Wellcome Trust Senior Research Fellow in Clinical Science at University of Oxford	NTL0030
	Dr Lisa Forsberg, British Academy Postdoctoral Fellow at University of Oxford	NTL0013 NTL0030
	Professor Simona Francese, Professor of Forensic and Bioanalytical Mass Spectrometry at Sheffield Hallam University	NTL0024
	Professor Pete Fussey, Professor of Sociology, University of Essex	NTL0017
	Professor Angela Gallop, Professor of Practice/Director of Forensic Science at University of Strathclyde/Forensic Access	NTL0024
**	Professor Colin Gavaghan, Director New Zealand Law Foundation Centre for Law and Policy in Emerging Technologies at University of Otago (QQ 39–51)	NTL0047

	Dr Jamie Grace, Senior Lecturer in Law at Sheffield Hallam University	NTL0001
	Professor Nigel Harvey, Professor of Judgment and Decision Research at UCL London	NTL0025
	Tobias Harvey, Student of Law at Kings College London	NTL0025
	Dr Binesh Hass, Research Fellow at University of Oxford	NTL0030
	The Home Office	NTL0055
	Independent Office for Police Conduct	NTL0054
	The Information Commissioner's Office (ICO)	NTL0016
	Istanbul Bar Association	NTL0028
*	Professor Elizabeth E Joh, Martin Luther King Jr. Professor of Law at University of California, Davis (QQ 39–51)	
	Perry Keller, Reader in Media and Information Law, Director of Doctoral Studies at King's College London	NTL0011
	Professor Paul Kelly, Professor of Inorganic Chemistry at University of Loughborough	NTL0024
	Professor Richard I.Kemp, Professor of Psychology at UNSW Sydney	NTL0012
	Dr Kyriakos N Kotsoglou, Senior Lecturer in Law, Northumbria University/Research Fellow, University of Lausanne	NTL0006 NTL0007
	The Law Society of England and Wales	NTL0023
	Dr Christopher Lawless, Associate Professor at Durham University	NTL0029
*	Dr David Leslie, Ethics Theme Lead at Alan Turing Institute (QQ 25–38)	
*	David Lewis, Former Deputy Chief Constable and former ethics lead NPCC at Dorset Police (QQ 68–82)	
	Liberty	NTL0020
	Sjors Ligthart LLM PhD candidate at Tilburg University	NTL0013
	Dr Nessa Lynch, Associate Professor of Law at Victoria University of Wellington	NTL0021
*	The Rt Hon Kit Malthouse MP, Minister of State for Crime and Policing at the Home Office and Ministry of Justice (QQ 99–111)	
	Stephen Mason, Associate Research Fellow, Institute of Advanced Legal Studies	NTL0002

	Dee Masters, Barristers at A1 Law Consultancy/Cloisters Chambers	NTL0019
	Professor Derek McAuley, Director of Horizon Digital Economy Research Institute at University of Nottingham	NTL0035
★★	Professor Carole McCartney, Professor of Law and Criminal Justice at Northumbria University (QQ 1–24)	NTL0022
	medConfidential	NTL0050
	The Metropolitan Police Service	NTL0031
	Professor Gerben Meynen, Professor of Forensic Psychiatry and Bioethics at Utrecht University and VU University Amsterdam	NTL0013
★★	Alun Michael, Police and Crime Commissioner for South Wales and Joint Lead for Data and Bioethics, Association of Police and Crime Commissioners (QQ 83–98)	NTL0049 NTL0057
	Migrants’ Rights Network	NTL0042
	The Ministry of Justice	NTL0053
	Abhishek Mishra, Doctoral Student at University of Oxford	NTL0030
	Dr Brent Mittelstadt of the Oxford Internet Institute (OII)	NTL0058
	Dr Reuben Moreton, Reli Ltd	NTL0026
	Professor Ruth Morgan, Professor of Crime and Forensic Sciences at University College London	NTL0024
	Dr Daragh Murray, Senior Lecturer in Human Rights at University of Essex	NTL0017
	NCC Group	NTL0005
	Dr Eilidh Noyes, University of Huddersfield	NTL0026
★	Dr Liam Owens, Founder and Chief Executive Officer, Semantics 21 (QQ 68–82)	
	Ms Angela Paul (PhD candidate in Law), Northumbria University	NTL0022
	Police Scotland	NTL0043
	Dr Susan Pope, DNA expert—chair of the Forensic Science Regulator DNA Specialist Group & is an assessor for the Netherlands Register of Court Experts at Principal Forensic Services	NTL0024
★★	Darryl Preston, Police and Crime Commissioner for Cambridgeshire and Peterborough and Joint Lead for Data and Bioethics, Association of Police and Crime Commissioners (QQ 83–98)	NTL0049 NTL0057

	Dr Christophe Prince, Director for Data and Identity, Home Office (QQ 99–111)	
	Privacy International	NTL0051
	Public Law Project	NTL0046 NTL0059
	Gary Pugh, Forensic Science Regulator	NTL0036
	Dr Jonathan Pugh, Parfit Radcliffe Senior Research Fellow at University of Oxford	NTL0030
	Dr Joe Purshouse, Senior Lecturer in Criminal Law and Justice at University of Sheffield	NTL0021
★★	Professor Charles Raab, Professorial Fellow, School of Social and Political Science, University of Edinburgh Fellow, The Alan Turing Institute (QQ 1–24)	NTL0014
	Dr Liam Ralph (Lecturer in Criminology and Policing) at the Centre for Crime and Policing & the Science and Justice Research, Northumbria University	NTL0022
	Dr Kay L. Ritchie, Senior Lecturer in Cognitive Psychology at University of Lincoln	NTL0003
	Royal Statistical Society	NTL0033
	Associate Professor. Mehera San Roque, UNSW Sydney	NTL0012
	SAS UK&I	NTL0041
	Professor Julian Savulescu, Professor of Practical Ethics at University of Oxford	NTL0030
	Serious Fraud Office	NTL0034
	Professor Ilina Singh, Professor of Neuroscience and Society at University of Oxford	NTL0030
	David Spreadborough, CFVA, Forensic Analyst at Amped Software	NTL0015
	Dr Amy Stevens, Senior Research Officer, Human Rights, Big Data and Technology Project at University of Essex	NTL0017
	Dr Clare Sutherland, Senior Lecturer at University of Aberdeen	NTL0012
★★	Professor Paul Taylor, Chief Scientific Adviser, National Police Chiefs' Council (QQ 83–98)	NTL0049 NTL0057
	Dr Alice Towler, Research Fellow at UNSW Sydney	NTL0012
★★	David Tucker, Faculty Lead on Crime and Criminal Justice, College of Policing (QQ 83–98)	NTL0057

	Professor Gillian Tully, Professor of Practice for Forensic Science Policy and Regulation at King’s College London	NTL0024
	UCL Centre for the Forensic Sciences	NTL0010
	Dr Lachlan Urquhart, Lecturer in Technology Law, and Co-Investigator of the UKRI Trustworthy Autonomous Systems Node in Governance and Regulation at School of Law University of Edinburgh	NTL0035
*	Dr Rosamunde Elise van Brakel, Co-Director, Surveillance Studies Network, Associate Professor Tilburg University/Vrije Universiteit Brussel (VUB) (QQ 39–51)	
**	Professor Sandra Wachter, Associate Professor and Senior Research Fellow at Oxford Internet Institute (OII), University of Oxford (QQ 68–82)	NTL0058
	Dr Adrian Weller, Principal Research Fellow in Machine Learning at the University of Cambridge	NTL0040
	Dr David White, Senior Lecturer at UNSW Sydney	NTL0012
	Dr Matthias Wienroth (Vice-Chancellor’s Senior Fellow in Criminology/Sociology), Northumbria University	NTL0022
	Professor Kim Wolff, Director King’s Forensics at King’s College London	NTL0024
*	Professor Michael Woodridge, Head of Department of Computer Science, Professor of Computer Science at University of Oxford (QQ 25–38)	
*	Professor Karen Yeung, Interdisciplinary Professorial Fellow in Law, Ethics and Informatics, Birmingham Law School at The University of Birmingham (QQ 52–67)	
	Dr Miri Zilka, Research Associate in Machine Learning at the University of Cambridge	NTL0040

APPENDIX 3: CALL FOR EVIDENCE

Scope of the inquiry

The Committee seeks to explore the use of new technologies in the application of the law and the experience of people currently or previously engaged with them.

New technologies include but are not limited to: machine-learning approaches; advanced algorithmic tools; artificial intelligence; and semi-autonomous or autonomous devices or systems. Application of the law includes activities to enforce, discover, deter, rehabilitate, or punish people who breach the law in a variety of contexts, as well as the prediction and prevention of future breaches.

Over the course of its inquiry, the Committee will notably discuss the existing legal and governance framework around the development and use of these new technologies, ethical issues raised by their use in the application of the law, as well as the lived experiences of end-users and citizens interacting with them. While the geographical scope of the inquiry is necessarily limited to England and Wales, the Committee also welcomes contributions related to the use of new technologies in the application of the law in devolved jurisdictions and overseas.

The Committee would like to hear from individuals and organisations with an interest, experience, or expertise in the use of new technologies in the application of the law. This is an open call for evidence and the Committee is also keen to hear from members of the public. Please bring it to the attention of anyone you know who might be interested.

Respondents are welcome to answer any or all of the questions set out below. Respondents are equally welcome to flag the importance of other issues related to the inquiry that are not covered in the questions below but which they think the Committee should consider in its work. The Committee is looking for pragmatic approaches to the issues presented by new technologies in the application of the law, so please provide practical examples where possible.

Questions

1. Do you know of technologies being used in the application of the law? Where? By whom? For what purpose?

2. What should new technologies used for the application of the law aim to achieve? In what instances is it acceptable for them to be used? Do these technologies work for their intended purposes, and are these purposes sufficiently understood?

3. Do new technologies used in the application of the law produce reliable outputs, and consistently so? How far do those who interact with these technologies (such as police officers, members of the judiciary, lawyers, and members of the public) understand how they work and how they should be used?

4. How do technologies impact upon the rule of law and trust in the rule of law and its application? Your answer could refer, for example, to issues of equality. How could any negative impacts be mitigated?

5. With regards to the use of these technologies, what costs could arise? Do the benefits outweigh these costs? Are safeguards needed to ensure that

technologies cannot be used to serve purposes incompatible with a democratic society?

6. What mechanisms should be introduced to monitor the deployment of new technologies? How can their performance be evaluated prior to deployment and while in use? Who should be accountable for the use of new technologies, and what accountability arrangements should be in place? What governance and oversight mechanisms should be in place?

7. How far does the existing legal framework around new technologies used in the application of the law support their ethical and effective use, now and in the future? What (if any) new legislation is required? How appropriate are current legal frameworks?

8. How can transparency be ensured when it comes to the use of these technologies, including regarding how they are purchased, how their results are interpreted, and in what ways they are used?

9. Are there relevant examples of good practices and lessons learnt from other fields or jurisdictions which should be considered?

10. This Committee aims to establish some guiding principles for the use of technologies in the application of the law. What principles would you recommend?

APPENDIX 4: ABBREVIATIONS, ACRONYMS AND TECHNICAL TERMS

ADM	Automated Decision Making
AFR	Automated Facial Recognition
AI	Artificial Intelligence
Algorithm	A series of instructions for performing a calculation or solving a problem, especially with a computer. They form the basis for everything a computer can do and are therefore a fundamental aspect of all AI systems.
APCC	Association of Police and Crime Commissioners
Artificial Intelligence	Machines that perform tasks normally performed by human intelligence, especially when the machines learn from data how to do those tasks.
Automated Decision Making	The process of making a decision by automated means without any human involvement. Decisions can be made based on factual data or inferred data.
Automated Facial Recognition	A technological solution matching biometric patterns to provide an assessment of whether two digital images depict the same person. When deployed in live settings, this technology is known as Live Facial Recognition.
BEIS	Department for Business, Energy & Industrial Strategy
DCMS	Department for Digital, Culture, Media & Sport
Data analysis	The process of combining data from a variety of sources and applying organisational, statistical, mathematical or machine learning calculations to retrieve data, find a pattern, produce a conclusion or make a prediction.
Explainability	The ability to explain how a specific outcome was reached.
HART	Harm Assessment Risk Tool (a predictor for reoffending rates that has been used by Durham Constabulary).
ICO	The Information Commissioner's Office
Information Commissioner's Office	The regulatory body for information rights
LFR	Live Facial Recognition
Live Facial Recognition	See Automated Facial Recognition
Machine learning	A branch of Artificial Intelligence that allows a system to learn and improve from examples without all its instructions being explicitly programmed.

ML	Machine Learning
NDAS	National Data Analytics Solution (a national analytics capability being developed by West Midlands Police in conjunction with the Home Office).
NPCC	National Police Chiefs' Council
PCC	Police and Crime Commissioner
PDS	Police Digital Service
WMP	West Midlands Police