Information Commissioner's Office

Response to the call for evidence by the House of Lords Justice and Home Affairs Committee on the use of new technologies in the application of the law[1]

About the ICO

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000, and the Environmental Communications Regulations 2003 (PECR), among other legislation.

2. The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

3. The Information Commissioner's Office (ICO) has set out its key technology areas of interest in its Technology Strategy 2018-2021,[2] making engagement with other regulators and stakeholders on these issues a priority. A large proportion of new technologies used in law enforcement will use personal data, so the ICO welcomes the opportunity to respond to this call for evidence. The ICO has also recently responded to the Joint Committee on Human Rights' call for evidence on the Police, Crime, Sentencing and Courts Bill.[3]

Technologies used in the application of the law

4. Law enforcement has always been exploring how new technologies can assist in identifying or deterring individuals who breach the law or in

[1] https://committees.parliament.uk/call-for-evidence/549

[2] https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf

[3] Legislative Scrutiny of the Policing, Crime, Sentencing and Courts Bill (ico.org.uk)

improving its engagement with the public, with data processing being at the centre of these processes.[4] The ICO believes new technologies used in the application of the law must be compliant with current legal frameworks including data protection.

5. Every technology can create benefits or risks depending on the context, governance and oversight measures, as well as its purpose. We believe technologies used in the context of law enforcement require particular scrutiny in terms of their efficacy and transparency before they are deployed.

6. Various technological deployments used by law enforcement intersect with the ICO's remit, from AI to biometrics and surveillance cameras. Following the call's steer, we outline below some of the new and emerging technologies the ICO has engaged with, while underlining this does not comprise an exhaustive list.

Live Facial Recognition (LFR)

7. The Commissioner has published her Opinion on the use of Live Facial Recognition technology (LFR) by law enforcement in public places[5] and the result of an ICO investigation on the same issue.[6]

8. LFR involves the real-time 'sensitive processing' of biometric data within the meaning of s35(8)(b) of the DPA 2018. The processing of digital images containing the faces of individuals (eg. images extracted from CCTV) whose facial features are measured by LFR software to produce a biometric template of each image, is followed by the cross-referencing of these templates with biometric templates extracted from the scanned faces of individuals on a watchlist. The watchlist is created by 'competent authorities' such as the police. After a facial match is suggested, human intervention is required to assess whether the match is correct and to determine the appropriate response. LFR is an area of high priority for the ICO.

9. The Commissioner has emphasised that for the 'sensitive processing' of personal data through LFR she expects controllers (eg. police forces) to clearly articulate the purpose of the processing and how this purpose meets the threshold of strict necessity. In order to meet this standard the controller must consider the proportionality of the processing and the availability of viable alternatives. Effectiveness is also a key consideration as the controller needs to demonstrate the technology will actually be able

[4] https://www.apccs.police.uk/media/4886/national-policing-digital-strategy-2020-2030.pdf
[5] https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
[6] https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

to serve the stated purpose and provide a demonstrable benefit to the public.

10. In general, the deployment of a new technology that processes personal data needs to be driven by the proven ability of that system to fulfil a specific and legitimate purpose, not by the mere availability of the technology itself.

Web scraping and ex-post Facial Recognition Technology (FRT)

11. In July 2020 the ICO and the Office for Australian Information Commissioner (OAIC) opened a joint investigation into the data processing practices of Clearview AI, a US based company that 'scraped' data and used Facial Recognition Technology (FRT) to identify individuals.[7] Web scraping is the process of using automated software to extract information from web pages and storing that information for further use. Clearview's facial recognition app allowed users to upload a photo of an individual and match it to photos of that person scraped from the internet.

Data Analytics

12. The ICO acknowledges the benefits that new technologies and data processing can offer law enforcement and in December 2020 it released a toolkit designed to help competent authorities comply with data protection when using data analytics.[8] The ICO has defined data analytics as the use of software to automatically discover patterns in data sets (where those data sets contain personal data) and use them to make predictions, classifications, or risk scores. A number of UK police forces appear to use data analytics, including Durham Constabulary,[9] West Midlands Police,[10] Avon & Somerset Constabulary,[11] and Essex Police.[12]

[7] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc

[8] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/ico-launches-tool-to-help-police-forces-using-data-analytics/

[9] The force has been using the Harm Assessment Risk Tool (HART) since 2017 to categorise offenders according to their risk of committing a crime in the next two years. For more: https://www.tandfonline.com/doi/pdf/10.1080/13600834.2018.1458455

[10] West Midlands Police is the lead force on the National Data Analytics Solution (NDAS), a partnership between UK police forces, the National Crime Agency and Accenture to develop a new analytics capability for UK law enforcement.

[11] According to a report by the Centre for Data Ethics and Innovation the force uses Qlik Sense, a tool that applies predictive modelling to produce individual risk-assessment and intelligence profiles. https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making/main-report-cdei-review-into-bias-in-algorithmic-decision-making

[12] https://www.essex.police.uk/police-forces/essex-police/areas/essex-police/au/about-us/privacy-notices/analytics-for-everyone-a4e/

13. The ICO has issued an enforcement notice in regard to the Metropolitan Police Service's Gang Matrix, and the Commissioner has welcomed the Met's commitment to work with us to ensure the Matrix is brought into compliance with data protection.[13] Despite their benefits the misapplication of data analytics tools that don't comply with data protection risks compromising the investigatory activity law enforcement may be undertaking.

R&D

14. The Home Office's Accelerated Capability Environment (ACE) unit, is powered by Vivace,[14] a consortium of security industry partners, and develops algorithmic tools to assist the detection of crime. One of the algorithmic tools developed to detect child abuse offenders was live tested by the National Crime Agency and the Metropolitan, Norfolk, Suffolk and Surrey police forces according to ACE's Annual Review 2019/2020.[15] We are also aware the Police Digital Service is running a Police Digital Garage with IBM.[16]

The purposes of personal data processing using new technologies

15. Clearly articulating the purpose of any processing of personal data is fundamental to ensuring there is clarity in terms of which part of the DPA 2018 controllers and processors will need to comply with. In the law enforcement context, the nature of the controller and the purpose of the processing (general processing or for law enforcement) determine the regime (Part 2 or Part 3 of the DPA respectively) that applies. Any processing carried out by a competent authority which is **not** for the primary purpose of law enforcement will be covered by the general processing regime under the UK GDPR (read with Part 2 of the DPA 2018).[17]

16. Section 31 of the DPA 2018 sets out what are considered law enforcement purposes: "The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

[13] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/information-commissioner-s-investigation-into-the-metropolitan-police-service/

[14] https://www.vivace.tech/

[15] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/932326/ACE_annual_review_2020.pdf

[16] https://pds.police.uk/digital-garage/

[17] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/

17. Competent authorities may need to outsource certain processing to private vendors. When these tasks serve general processes such as HR or research, they fall under Part 2 of the DPA 2018 for general processing, not Part 3.

18. The ICO appreciates there may be uncertainty in terms of purpose but also in terms of the delegation of processor/controller responsibilities. Particular attention needs to be paid in the context of competent authorities commissioning private vendors to process personal data to develop and train algorithmic systems.

19. We would like to acknowledge that a 2019 report by the Law Society on the use of algorithmic systems in the justice sector recommended the ICO should produce guidance on how Part 3 functions in the context of public-private partnerships.[18]

20. It is important for law enforcement agencies to be mindful of the fact purpose limitation is a core principle of data protection. According to s.36 of Chapter 2 of Part 3 of the DPA 2018, the second data protection principle is that:

- the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;
- personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

Impact upon the rule of law, trust in the rule of law and mitigation of negative impacts

21. New technologies can provide significant benefits for law enforcement but their deployment needs to be compliant with data protection. The ICO recognised the changes technology can bring to the legal and societal environment and in 2018 it published its Technology Strategy. AI and big data was one of our priority areas so we welcome the call's focus on automation and algorithmic processes.

22. The increasing use of automation in decision-making through the use of algorithmic systems can have an impact on the rule of law and the public's trust in it. In general, new technologies can raise emergent risks and challenges that we briefly touch upon below.

Fairness in algorithmic decision-making

[18] https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report

23. Biased algorithmic systems, lack of transparency, accountability gaps and the inherent information asymmetry between controllers (eg. AI developers or vendors) and data subjects or decision-makers whose final decision systems are meant to inform, mean this technology has raised a series of complex questions in relation to how fair its deployment is and its overall impact upon the rule of law. The ICO intends to undertake work on the issue of fairness in algorithmic decision-making and is aware other regulators such as the Equality and Human Rights Commission (EHRC) are planning complementary work.

The importance of human review

24. We believe human oversight remains a fundamental factor in appropriating responsibility and retaining trust in new technologies and the sectors that use them. The ICO's Guidance on AI and Data Protection[19] proposes measures to ensure the results of algorithmic systems are appropriately scrutinised. There are three main considerations towards that goal:

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

The risk mitigation role of Data Protection Impact Assessments

25. We believe Data Protection Impact Assessments (DPIAs) provide a useful mechanism to monitor new technologies, and contribute to an evaluation of their performance while identifying and mitigating risks.

26. ICO guidance has explained that in the case of most AI systems and new technologies a DPIA will be mandatory to mitigate negative impacts, including risks to the rights and freedoms of individuals. The UK GDPR states that DPIAs are required (at least):

- before the deployment of innovative technological solutions;
- for the processing of special category personal data at large scale; or

[19] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection

- for automated decision-making, profiling, of for the expected denial of a service to an individual.[20]

27. The ICO has also emphasized that DPIAs should not be seen as an one-off exercise but 'live' documents that need to be kept under review and reassessed if anything changes.[21] We consider the publication of DPIAs a good way for controllers to demonstrate they are compliant with data protection.

Data protection by design

28. We believe organisations internalising the principle of data protection by design and by default[22] would bolster accountability and mitigate risks at the design stage. The importance of considering data protection early in the development stage was also highlighted in our Investigation Report on Mobile Phone Data Extraction by Police Forces in England and Wales.[23]

Costs, benefits and safeguards to ensure compatibility with a democratic society

29. The requirements of fairness, necessity and proportionality under data protection law reflect the fact that innovative, new ways of processing personal data can involve both costs and benefits. The ICO has raised the risk of encoding bias in algorithmic systems (including those used in law enforcement) and broader risks to rights and freedoms. We believe a robust data protection framework and an empowered and appropriately resourced data protection regulator are important to protect the safeguards required in a democratic society.

The existing legal framework: data protection and law enforcement

30. The ICO is the UK's data protection regulator and in that context it is exclusively concerned with technologies that process personal data. The DPA 2018 sets out the legal framework for data protection law in the UK and it sits alongside and supplements the UK GDPR.

31. Part 3 of the DPA 2018 sets out a separate data protection regime for 'competent authorities' with law enforcement functions when they are processing for law enforcement purposes. Part 3 and its provisions apply only to competent authorities as listed in Schedule 7 of the DPA.[24] It applies for example, to the police, criminal courts, prisons, non-policing

[20] https://ico.org.uk/about-the-ico/news-and-events/ai-blog-data-protection-impact-assessments-and-ai/

[21] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

[22] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[23] Mobile phone data extraction by police forces in England and Wales (ico.org.uk)

[24] https://www.legislation.gov.uk/ukpga/2018/12/schedule/7/enacted

law enforcement. It also applies to relevant processors when undertaking law enforcement processing.

32. The ICO has emphasized that data protection law does not exist in a vacuum. Other legal obligations such as complying with the Public Sector Equality Duty (PSED) under s.149 of the Equality Act 2010, may also need to be considered when deploying new technologies depending on the context. We are also aware the Law Commission is considering automated decision-making in its 14th Programme for law reform and the ICO has engaged with the Commission on this matter.[25]

Ensuring transparency

33. Transparency in terms of procurement and supply chain issues that influence how the responsibilities of controller and processor are allocated are an issue of increasing interest for the ICO. Data protection already includes documentation requirements whenever processing of personal data is involved under Article 30(1) of the UK GDPR.

34. While the processing undertaken by law enforcement does not include an obligation to meet the same standards on transparency towards the affected citizens that Articles 13-15 of UK GDPR stipulate, it is in the ICO's view an important requirement for law enforcement to consider how to inform the data subjects of decisions that have been made using automated means. In this context, we support efforts such as the decision by the Ministry of Justice to publish details of a recidivism scoring system.[26]

35. The ICO has published guidance on Explaining Decisions Made with AI,[27] co-authored with the Alan Turing Institute that explains how organisations can embed the principle of transparency in the development and deployment phases of their systems.

Good practices and lessons learnt from other fields or jurisdictions

36. Even though confidentiality is a necessary element of various law enforcement functions, enhanced transparency via a register of algorithmic and data analytics systems used by law enforcement could be something to consider. The cities of Amsterdam and Helsinki have already launched algorithmic registers and the EU proposed Artificial Intelligence Act also includes provisions for a register of high-risk systems. The ICO

[25] https://www.lawcom.gov.uk/14th-programme-kite-flying-document/

[26] A compendium of research and analysis on the Offender Assessment System (OASys), 2009–2013 (publishing.service.gov.uk)

[27] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/

has expressed its support for the latter proposal in its response to the EU AIA consultation.[28]

37. The ICO finds that the direction of travel in terms of regulating emerging technologies appears to be ex-ante measures that look upstream in the pipeline. This perspective is reflected in our work on the ICO's AI and Data Protection Risk Mitigation and Management Toolkit[29] as well our internal AI Auditing Toolkit.

38. The ICO's Regulatory Sandbox has also provided a useful environment to innovative companies to test their products and we are looking forward to doing more work in this space.

Guiding principles for the use of technologies in the application of the law

39. Data protection law is aiming to protect not just individual rights to data protection but fundamental rights more broadly. At the same time, core data protection principles such lawfulness, transparency and fairness, accountability, and accuracy are particularly pertinent in the law enforcement context.

40. The ICO would like to bring to the Committee's attention the fact the Global Privacy Assembly's (GPA) International Enforcement Working Group (IEWG)[30] that the ICO currently co-chairs is working on the development of privacy principles and expectations for the use of personal data in FRT.

41. We believe data protection principles such as fairness, transparency, accountability and accuracy should be considered as guiding principles for the use of technologies in the application of the law.

	Response to the House of Lords Justice and Home Affairs Committee call for evidence on the use of new technologies in law enforcement
Date	02–09-2021
Submitted by	The Information Commissioner's Office

[28] ico-response-eu-artificial-intelligence-act-20210728.pdf

[29] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ai-and-data-protection-risk-mitigation-and-management-toolkit

[30] https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2d-Day-3-3_2e-v1_0-International-Enforcement-Cooperation-Working-Group-Report-Final.pdf