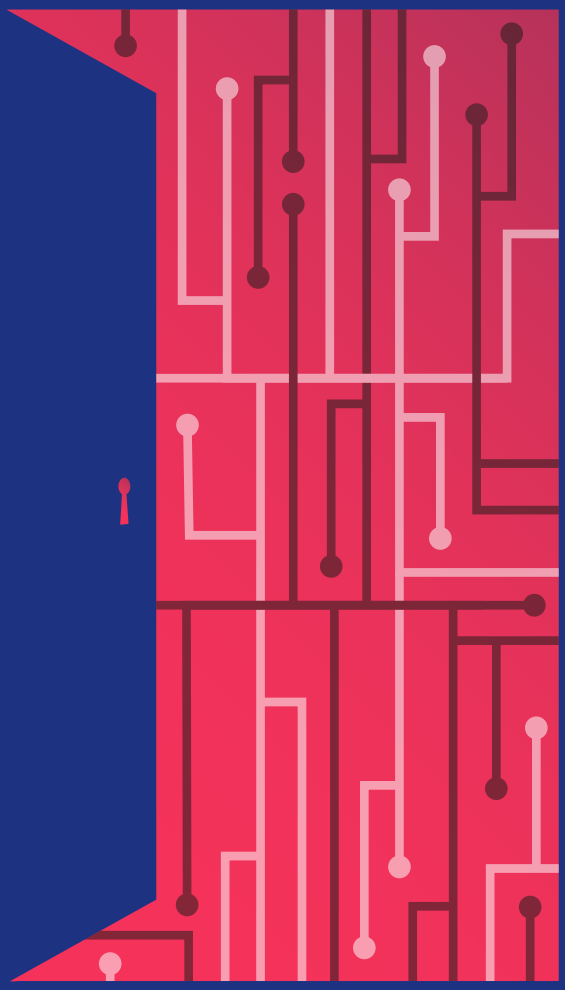


ARTIFICIAL INTELLIGENCE AGENCIES:

The Use and Regulation of AI in UK Intelligence Agencies

November 2026

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

DISCLAIMER

Privacy International observes the greatest possible care in using information and drafting publications, including vetting sources relied upon, but cannot guarantee that this report is complete and there are no errors in the sources used. The report is provided for informational purposes and is not to be read as providing endorsements, representations or warranties of any kind whatsoever. Opinions and information provided are made as of early August 2026 and are subject to change without notice.

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission.This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 4.0. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence: info@privacyinternational.org

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Privacy International
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

CONTENTS

EXECUTIVE SUMMARY 6

INTRODUCTION 10

DEFINING AI 12

1. HOW ARE UK INTELLIGENCE AGENCIES USING ARTIFICIAL INTELLIGENCE? 15

1.1 Introduction 16

1.2 How are UK intelligence agencies using AI? 18

AI Infrastructure 19

Collecting Data 20

Analysing the Data 21

1.3 Why is the use of AI in intelligence contexts harmful? 26

Secrecy: National Security, AI, and State Secrets 26

Surveillance at Scale 28

Making sense of it all 33

Predictive "Intelligence" 34

The prevalence of errors and bias 35

Opaque Reasoning 37

2. HOW IS AI USE BY INTELLIGENCE AGENCIES REGULATED IN THE UNITED KINGDOM? 40

2.1 Introduction 41

General Overview 41

2.2 Understanding the Regulation **46**

Data Protection Law 46

The application of data protection laws to intelligence agencies 48

The national security exemption 49

The security breach notification gap 52

Human Rights and Equality laws 54

The application of human rights and equality laws to intelligence agencies 57

The national security exemption 57

Challenges with bringing a claim under equality law 59

Bringing a claim under the Human Rights Act 59

Facial Recognition Technology as a Case Study 62

Intelligence laws 64

How the Investigatory Powers Act governs AI 66

2.3 Unpacking Specific Regulatory Challenges and Gaps **69**

No interrogation of AI involvement or duty to disclose 69

The urgency carve-out 71

Datasets with a low or no expectation of privacy 72

Third party bulk personal datasets 75

Technical Capability Notices 77

Bulk Surveillance: Authorising "Selectors" 80

Examination warrants 83

The National Security Exemption 85

Scope creep 85

Deference 87

3. WHAT SHOULD BE DONE? 91

3.1 Introduction 92

3.2 Prohibited Uses 94

3.3 Stage 1 – Data Collection 96

Principles applicable to all warrants and authorisations 96

Targeted Warrants and Authorisations 97

Bulk Warrants 98

Problematic Collection Outside of the Warranty Process 99

3.4 Stage 2 – Making the Data Useable 101

Combining Data 101

AgenticAI 102

3.5 Stage 3 – Using the Data 103

Examination 103

Logging, Audits and Transparency 105

Training Data 106

Oversight and Redress 106

3.6 National Security Exemptions from Data Protection Requirements 109

CONCLUSION 111

Appendix 1 : The AI Pipeline & Use Cases 112

Appendix 2 : Condensed Findings 121

EXECUTIVE SUMMARY

1. In the halls of MI6 and GCHQ, like in intelligence agencies all over the world, artificial intelligence (AI) has become a fundamental part of the workflow. But how are intelligence agencies wielding these powerful technologies, and what policies guide their use? Our research attempts to understand this by looking at two questions. First, how are intelligence agencies using AI? And second, how is that use regulated in the United Kingdom?

2. Intelligence agencies are eager to signal that they are using AI but are careful not to reveal exactly what they are up to. As a result, we are left attempting to surmise, piece-meal, by relying on leaked documents, extrapolating from publicly known commercial capabilities and reading between the lines of cryptic procurement requests and public-facing policy documents, how intelligence agencies are using AI and what risks their use poses to our rights. We know that intelligence agencies are using AI to gather and make sense of vast quantities of public and private data, in addition to data collected by private companies, but which can be sold to or shared with the government. Intelligence agencies have myriad use cases for this data – from mapping relationships, to targeting individuals in armed conflicts, to predicting threats. We do not know how many people these systems affect, how these AI systems were trained, or how much faith intelligence agencies place in them. Many questions are left unanswered, and national security exemptions often mean that intelligence agencies are not under any legal obligation to answer them.

3. The UK lacks a comprehensive AI law and instead uses a fragmented, cross-sectoral regulatory framework to govern AI use, including by its intelligence agencies.

4. Data protection law plays an important role in the regulation of AI, where AI processes personal data. It does so through the application of data protection principles, and the provision of certain rights – particularly rights related to automated decision-making. However, intelligence agencies are not required to comply with data protection law when acting to safeguard national security. Insufficient legal certainty is provided about when a national security exemption may apply.

5. Human rights and equality laws safeguard human rights, including the right to privacy, and guard against discrimination as a consequence of AI use by public authorities. But their application to intelligence services may be limited in the context of national security.

6. The UK has a set of sector specific laws, including the Investigatory Powers Act 2016, which govern the intelligence agencies, but none of them explicitly address AI use.

7. UK intelligence law is thus complex and fragmented. It is further limited because it does not equally apply to every stage of the "AI pipeline", which includes: stage 1 - data collection; stage 2 - making the data useable; and stage 3 – using the data. Stage 1 – data collection, is the most comprehensively regulated, and even so, fails to effectively regulate how intelligence agencies collect data both using AI, and for AI to use. Key risks posed by the current UK regulatory regime include:

7.1 Key risks in stage 1 – data collection: there is no requirement to disclose or scrutinise AI involvement in warrant applications; warrant authorisers are not required to interrogate AI involvement, AI outputs, or reliability; and authorisation and oversight of bulk warrants leave even less room for scrutiny. These gaps mean that AI-generated intelligence may be opaque and insufficiently vetted.

7.2 AI use also compounds already problematics gaps in warrant authorisation processes, including: urgency powers which allow data collection before approval from a Judicial Commissioner, but don't mandate deletion if approval is later denied; the collection of a new category of datasets – those with low or no reasonable expectation of privacy – which are loosely defined and unlikely to remain a low risk to privacy when AI processing is applied; and access before authorisation for third-party datasets which creates a regulatory loophole which could be exploited with advancing AI.

7.3 **Key risks in stage 2 – making the data useable:** data from different warrants can be combined without additional authorisation; risks from merging datasets include: amplification of bias, false correlations, intrusive profiling, and re-identification of anonymised data. Existing safeguards do not adequately address these risks, and no safeguards explicitly cover data integration, preprocessing, or dataset merging.

7.4 **Key risks in stage 3 – using the data:** once data is collected, especially in bulk, it is analysed and examined. Current safeguards designed to protect our rights in this process, including by the

authorisation of selectors and examination warrants, are undermined by the new power of AI. Warrants may also permit use for testing or training, implicitly allowing collection for AI development; no legal framework exists to restrict high-risk AI uses.

7.5 Broad national security exemptions exist across all of the regulatory frameworks we consider. They can be used to exempt compliance with regulations and safeguards which are attempting to grapple with AI use and permit action where it would otherwise be unlawful. Whether a national security exemption applies is often discretionary. The scope of national security is undefined, broad, and highly flexible, which enables inconsistent application and scope creep. Oversight mechanisms give a large degree of deference to executive decisions, limiting meaningful review and risk becoming "legal grey holes" – strong in theory but weak in practice.

8. We conclude with recommendations for how UK regulation of AI use by intelligence agencies could be improved, both by increasing the effectiveness of certain safeguards and drawing clear lines where AI should be prohibited, especially when it comes to automated decision making.

INTRODUCTION

In December 2025, the new chief of the Secret Intelligence Services (MI6), Blaise Metreweli remarked that:[1]

> *"[t]he defining challenge of the twenty-first century is not simply who wields the most powerful technologies, but who guides them with the greatest wisdom. Our security, our prosperity, and our humanity depend on it."*

But how are intelligence agencies wielding these powerful technologies, and what guides their use?

Our research attempts to answer two questions. First, how are intelligence agencies in the United Kingdom (UK), and elsewhere, using artificial intelligence (AI)? And second, how is that use regulated? We say 'attempts' because the information needed to answer these questions is hard to find. We anticipated this. The conduct of intelligence agencies is notoriously opaque. An occupational requirement, they often justifiably say.[2] But this opacity is an obstacle for both democratic accountability[3] and redress when abuse does occur.[4]

What we did find reveals that intelligence agencies are likely using AI in several ways, including to gather and make sense of vast quantities of public and private data. This data is analysed to map relationships, predict threats, and

1 Foreign, Commonwealth & Development Office, Secret Intelligence Service, 'Speech by Blaise Metreweli, Chief of SIS', 15 December 2025, available at: https://www.gov.uk/government/speeches/speech-by-blaise-metreweli-chief-of-sis-15-december-2025.

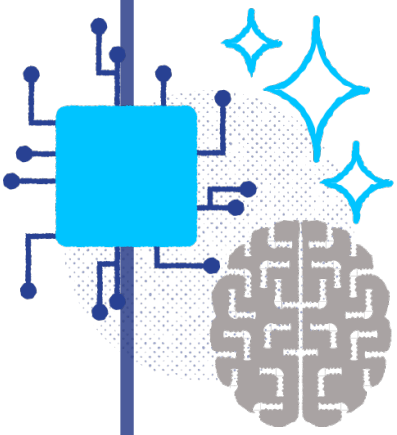
2 Richard Moore of MI6 briefly remarked on this so-called occupational requirement in an address, noting: "we have to maintain secrecy not as an end in itself but because the lives of our agents and the effectiveness of our work depend on it". WATCH: MI6 boss Richard Moore on global security, Ukraine war and impact of AI, [4:56] Politico Europe, 19 July 2023, available at: https://www.youtube.com/watch?v=5PWH7HX1Rcc.

3 David Andersen Q.C, Intendent Reviewer of Terrorism Legislation, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015, available at: https://assets.publishing.service.gov.uk/media/5a7f9b66ed915d74e622b7ca/IPR-Report-Web-Accessible1.pdf.

4 Some of Privacy International's previous work highlights unlawful conduct that was previously secret. See, e.g., 'Press release: UK intelligence agency admits unlawfully spying on Privacy International', Privacy International, 25 September 2018, available at: https://privacyinternational.org/press-release/2283/press-release-uk-intelligence-agency-admits-unlawfully-spying-privacy; 'MI5 Ungoverned Spaces Challenge', Privacy International, 30 January 2023, available at: https://privacyinternational.org/legal-action/mi5-ungoverned-spaces-challenge.

target the individuals posing those threats, including in armed conflicts.

Our review of the regulatory framework as applied to intelligence agencies, including the Security Service (MI5), the Secret Intelligence Service (MI6) and Government Communications Headquarters (GCHQ), reveals that broad national security exemptions undermine many existing safeguards. Recent amendments to the Investigatory Powers Act 2016 seem to enable the use of AI and its mass data requirements but provide insufficient safeguards to mitigate the risks. As such, we conclude our report with a set of proposed recommendations that aim to improve regulation by increasing the efficacy of certain existing safeguards, and to draw clear lines where AI should be prohibited.



DEFINING AI

Effective regulation of the advanced AI techniques discussed in this paper should start with a definition of what 'AI' is being regulated. This is not an easy question to answer, as the technology is rapidly changing.

The UK's Investigatory Powers Commissioner's Office (IPCO) promulgated the following definition in its AI Scope of Interest:[5]

"An 'AI system' is a collection of software components that together have one or more of the following features:

- *Uses data science techniques in the processing of large volumes of information;*
- *Can operate without direct human control in a partially or fully autonomous manner, including making decisions or selections;*
- *Can adapt its functions or outputs based on new information;*
- *Can generate new information such as text, sound or images.*

The software may or may not be specifically described by its developers as 'AI' technology, but if its effect is, or is expected, to significantly change the breadth and/or depth of intrusions to privacy, and it has at least one of the features described in 2(a-d) above, then it should be treated as an AI system".

The International AI Safety Report[6] provides another useful example with its description of *"general-purpose AI"* as

5 Investigatory Powers Commissioner's Office, 'IPCO'S Scope of Interest in AI', 26 March 2025, available at: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCOs-Scope-of-Interest-in-AI.pdf.

6 International AI Safety Report 2026, 3 February 2026, available at: https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026#1-background-on-general-purpose-ai.

> *"AI models and systems that can perform a variety of tasks, rather than being specialised for one specific function or domain,"*[7] *and are "based on 'deep-learning'", which "involves using large amounts of computational resources to help AI models learn complex relationships and abstract features."*[8]

Similarly, the United Nations' Independent International Scientific Panel on AI describes the AI it focuses on as:[9]

> *"machine systems that, broadly speaking, perceive, learn and act. They infer from inputs how to generate outputs such as predictions, content, recommendations, actions or decisions, with varying degrees of autonomy and adaptiveness. What unifies current AI more than any single architecture is that modern systems learn from experience represented by data."*

The UN Panel further explains that while general-purpose AI is the current focus of much public discussion, and their analysis, task-specific AI systems also exist and are advancing. A task-specific system is designed to perform tasks in specific domains, and:[10]

> *"delivers measurable benefits when the task is well defined, the data are available and institutions can deliberately deploy it."*

All three of these AI definitions share common components, including:

- relying on the processing and use of large amounts of data and computational resources;
- to perform a breadth of tasks, including being able to learn, adapt and act, with varying degrees of autonomy including by making automated decisions;

7 Ibid., p. 11.

8 Ibid., p. 17.

9 The United Nations' Independent International Scientific Panel on AI, 'Preliminary Report of the Independent International Scientific Panel on AI', July 2026, available at: https://www.un.org/independent-international-scientific-panel-ai/sites/default/files/2026-07/en_Preliminary%20Report_.pdf, p. 11.

10 Ibid.

- which results in the generation of new information, often probabilistic in nature.

For the purposes of this paper, we consider systems with these features to be 'AI'.

As the IPCO points out, systems with these features may not be explicitly described as 'AI', but if a system's effect is to increase the breadth or depth of the privacy intrusion and has the above features, it should be considered AI for the purposes of this paper.[11]

Further, agentic-AI is a type of AI that the UN describes as a *"qualitative step change."*[12] The French data protection authority, CNIL, described agentic-AI as:[13]

> *"a set of computer programs built on generative AI models capable of autonomous decisions, orchestration of complex actions, and interaction with third-party services, with or without human validation".*

While a full exploration of the effect of agentic-AI on intelligence gathering is beyond the scope of this paper, we touch on some aspects of its use and regulation.

11 IPCO, (n 5), p. 2.

12 Preliminary Report of the Independent International Scientific Panel on AI, (n 9), § 6.2.

13 Jadzia Pierce, 'French CNIL Publishes Note on Agentic AI and Data Protection' (Covington, 13 August 2026) available at: https://www.insideprivacy.com/artificial-intelligence/french-cnil-publishes-note-on-agentic-ai-and-data-protection/.

1. HOW ARE UK INTELLIGENCE AGENCIES USING ARTIFICIAL INTELLIGENCE?

1.1 INTRODUCTION



Intelligence agencies have rapidly adopted advanced forms of AI over the last decade.

Leaders in the intelligence space from around the globe, including the former heads of the US's CIA and the UK's MI6, have boasted about their respective AI capabilities, and promised to continue adopting new AI technology at breakneck speed.[14]

It is likely that most governments around the world are using AI in domestic and international intelligence operations. Their intelligence agencies are using national security and counter-terrorism narratives as a reason to adopt it.[15] Further, world leaders have come to view the advancement and integration of AI into the intelligence sphere as imperative to remaining militarily and economically competitive on a global scale.[16]

It is next to impossible, however, for lay people, even highly skilled investigative reporters and researchers, to figure out exactly how intelligence agencies are using AI.[17] The information that is available suggests that intelligence agencies may be using AI to: enhance military capabilities

14 Laura Dobberstein, 'MI6, CIA using generative AI to combat tech-driven enemies' (The Register, 9 September 2024) available at: https://www.theregister.com/2024/09/09/mi6_cia_genai/; see also, 'CIA director Bill Burns and MI6 chief Richard Moore talk to FT editor Roula Khalaf' (FT Live, 7 September 2024) available at: https://www.youtube.com/watch?app=desktop&v=rp5PeoAW6mI&cbrd=1.

15 United Nations Human Rights Council, Report A/HRC/52/39, available at: https://docs.un.org/en/A/HRC/52/39, para 9.

16 Antoaneta Roussi, 'UK MI6 using artificial intelligence to counter China, says Richard Moore' (Politico, 19 July 2023) available at: https://www.politico.eu/article/uk-mi6-artificial-intelligence-counter-china-richard-moore/; Jared Dunmon, 'The Real Threat of Chinese AI' Foreign Affairs' (Foreign Affairs, 28 February 2025) available at: https://www.foreignaffairs.com/china/real-threat-chinese-ai.

17 See, e.g., Faiza Patel and Patrick Toomey, 'Bringing transparency to national security uses of artificial intelligence' (Brennan Center for Justice, 9 April 2024) available at: https://www.brennancenter.org/our-work/analysis-opinion/bringing-transparency-national-security-uses-artificial-intelligence.

through AI targeting and autonomous weapons;[18] carry out cyber espionage and cyber-attacks;[19] surveil and monitor individuals both inside and outside of a country's jurisdiction, including through the use of facial recognition technology (FRT);[20] collect and analyse data and make conclusions about the threat to national security an individual, group, or ideology poses;[21] make predictions about whether, when, and where individuals might commit a crime;[22] and monitor the media, control narratives, and create deepfakes.[23]

This report is primarily concerned with the legal implications of the ways intelligence agencies in the UK may use AI to surveil, monitor, profile and make predictions about individuals and communities. The following sections discuss what we know, or can infer, about those uses and the human rights harms they may cause.

18 Amos Toh and Emile Ayoub, 'The military's use of AI explained' (Brennan Center for Justice, 12 March 2026) available at: https://www.brennancenter.org/our-work/research-reports/militarys-use-ai-explained.

19 Paul J and Alan Steer, 'Why cyber defenders need to be ready for frontier AI' (National Cyber Security Centre, 30 March 2026) available at: https://www.ncsc.gov.uk/blogs/why-cyber-defenders-need-to-be-ready-for-frontier-ai; Morgan Adamski, David Ames, and Rob Joyce, 'AI-orchestrated cyberattacks: A new cybersecurity threat landscape' (PricewaterhouseCoopers, 14 November 2025) available at: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/ai-orchestrated-cyberattacks.html.

20 Jay Stanley, 'Machine surveillance is being supercharged by large AI models' (ACLU Speech, Privacy, and Technology Project, 21 March 2025) available at: https://www.aclu.org/news/privacy-technology/machine-surveillance-is-being-super-charged-by-large-ai-models; Mehul Srivasta and Christopher Miller, 'New AI espionage powers trigger Putin camera scare' (The Financial Times, 9 June 2026) available at: https://www.ft.com/content/6f4d806c-eb22-4c32-8352-b82692d30e9f?accessToken=zwAAAZ6xxR49kc9vTYBs6yJMMtODUrgmktMOnw.MEQCIElWEd1jfKP-sBck-CZVi_-0B1CnSrktvaBzF-1V70CfAiAzphdWPLZ5S71d6n7kSLODcWLO5xWD5sNy0UIPRQi_rA&sharetype=gift&token=1210405a-3467-474f-8d5d-963b1429e3f9&syn-25a6b1a6=1.

21 'How spy agencies are experimenting with the newest AI models' (The Economist, 29 July 2025) available at: https://www.economist.com/international/2025/07/29/how-spy-agencies-are-experimenting-with-the-newest-ai-models.

22 Rachel Levinson-Waldman and Ivey Dyson, 'The dangers of unregulated AI policing' (Brennan Center for Justice, 20 November 2025) available at: https://www.brennancenter.org/our-work/research-reports/dangers-unregulated-ai-policing.

23 Aryamehr Fattahi, 'AI-driven information warfare, disinformation and psychological manipulation' (Bloomsbury Intelligence and Security Institute, 8 December 2025) available at: https://bisi.org.uk/reports/ai-driven-information-warfare-disinformation-and-psychological-manipulation.

1.2 HOW ARE UK INTELLIGENCE AGENCIES USING AI?

Information about how the UK intelligence agencies use AI is hard to come by. The UK exempts all intelligence agencies, including MI5, MI6, GCHQ, Defence Intelligence, and the National Crime Agency, from Freedom of Information Requests (FOI), and these agencies have largely refrained from disclosing in detail how they are using AI. Intelligence services in the UK are overseen by the Intelligence and Security Committee of Parliament, the Information Commissioner's Office (ICO), the Investigatory Powers Commissioner's Office (IPCO) and the Investigatory Powers Tribunal (IPT).[24] All three of these regulatory agencies have acknowledged that public sector use of AI is a cause for concern.[25] Sharing that concern, the following section outlines what we have been able to gather about intelligence agencies' use of AI. Some of it is UK-specific, but we include examples from around the world to try to build as detailed a picture as possible of how AI is being used.

The UK has made it clear that it is employing AI in intelligence contexts. In September 2024, Richard Moore, former-chief of the UK MI6 gave a joint interview with the head of the CIA and emphasized the importance of integrating technology into MI6:

> *"we are now using AI, including generative AI, to enable and improve intelligence activities — from summarisation to ideation to helping identify key information in a sea of data. We are training AI to help protect and 'red team' our own operations to ensure we can still stay secret when we need to. We are using cloud technologies so our brilliant data scientists can make the most of our data, and we are partnering with the most innovative companies in the US, UK and*

24 'How we work: law, oversight and ethics' (MI5) available at: https://www.mi5.gov.uk/how-we-work/law-oversight-and-ethics, accessed 10 September 2026.

25 'Annual Report of the Investigatory Powers Commissioner 2024' (IPCO, 16 December 2025) available at: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2024.pdf, p. 7; see also, IPCO Scope of Interest in AI (n 5).

around the world."[26] *Later, Richard Moore wrote in Politico: "Control of data is vital for national sovereignty," and the UK must learn how to master AI technology because its adversaries are doing the same."*[27]

AI Infrastructure

This desire for control is manifesting in the UK government making significant investments in infrastructure to support AI use for intelligence purposes. For instance, the National Security Strategic Investment Fund (NSSIF) has been investing in start-up technology for years. But in July 2025, the UK government began to promote the fund more publicly, and allocated to it an additional £330 million over four years to focus on the 'critical intersection' of dual use technologies, which may include AI, and national security.[28] In 2021, the Financial Times reported that the Government contracted with Amazon Web Services to host data for UK intelligence agencies.[29] Such data, as discussed in the next section, is the foundation for AI applications. Outside of the intelligence realm, in 2025, the UK signed a deal with Open AI called 'stargate UK' to strengthen the UK's sovereign computing capabilities to run *"world-leading AI models"*.[30]

The United States has similarly been expanding its access to advanced AI and *"compute"*, which is the term for data centre infrastructure and chips on which AI systems rely. According to the New York Times, the Trump Administration approved USD$9 billion to procure AI compute, alongside USD$800m for computing capacity.[31]

26 Bill Burns and Richard Moore, 'Intelligence Partnership Helps the US and UK Stay Ahead in an Uncertain World' (The FT, 7 September 2024) available at: https://www.ft.com/content/252d7cc6-27de-46c0-9697-f3eb04888e70.

27 A. Roussi,'UK MI6 using AI to Counter China' (n 16); L. Doberstein, MI6, CIA using generative AI to combat tech-driven enemies (n 14).

28 Joseph Bambridge, 'Britain's secretive spy fund out shadows NSSIF, GCHQ, MI5, MI6' (Politico, 16 July 2025) available at: https://www.politico.eu/article/britain-secretive-spy-fund-out-shadows-nssif-gchq-mi5-mi6/.

29 Helen Warrell and Nic Fildes, 'Amazon Web Services contract for data with MI5, MI6 and GCHQ' (The Guardian, 26 October 2021) available at: https://www.theguardian.com/uk-news/2021/oct/26/amazon-web-services-aws-contract-data-mi5-mi6-gchq.

30 'Introducing Stargate UK' (OpenAI, 16 September 2025) available at: https://openai.com/index/introducing-stargate-uk/.

31 Dustin Volz and Julian E. Barnes, 'White House Approves $9 Billion for Spy Agencies to Catch Up on A.I.' (The New York Times, 22 May 2026) available at: https://www.nytimes.com/2026/05/22/us/politics/spy-agencies-ai-chips-shortage.html?searchResultPosition=2.

Collecting Data

Governments are designing infrastructure to facilitate the storage and processing of vast amounts of information, which, intelligence services are also increasingly collecting. For example, under the Trump Administration, the US has moved to collect and analyse data for border and immigration policing. Social media monitoring in early 2025 was reportedly used for an 'AI-fuelled Catch and Revoke' to review student visa holders' social media accounts.[32] The Administration then sought to expand the collection of social media data from all non-residents.[33] Over the last two years Immigration and Customs Enforcement has accumulated vast amounts of data to conduct their operations,[34] and uses tools including facial recognition,[35] mobile phone tracking,[36] and predictive software[37] that recommends where the agency should direct enforcement activities.

In a dispute between the US Department of Defence (DoD) and Anthropic, whose AI models the DoD were using on classified systems, it emerged, according to the New York Times, that the Pentagon wanted to use Anthropic's technology to assist with *"the collection and analysis of unclassified, commercial bulk data on Americans, such as geolocation and web browsing data."*[38] It is unclear how effectively US law would prevent such mass surveillance, including of US persons, either based on purchased commercial

32 Kanishka Singh, 'Rights advocates concerned by reported US plan to use AI to revoke student visas (Reuters, 7 March 2025) available at: https://www.reuters.com/technology/artificial-intelligence/us-use-ai-revoke-visas-students-perceived-hamas-supporters-axios-reports-2025-03-06/.

33 'The Trump Administration wants your DNA and social media (Privacy International, 11 December 2025) available at: https://privacyinternational.org/news-analysis/5713/trump-administration-wants-your-dna-and-social-media.

34 Peter Andringa, 'Trump's immigration data dragnet' (The FT, 10 December 2025) available at: https://ig.ft.com/us-ice-surveillance/.

35 Dave Mass, 'Rights Organisations Deman Halt to Mobile Fortify, ICE's Handheld Face Recognition Program' (Electronic Frontier Foundation, 26 November 2025) available at: https://www.eff.org/deeplinks/2025/11/rights-organizations-demand-halt-mobile-fortify-ices-handheld-face-recognition.

36 Lucy Hay Newman and Matt Burgess, 'Security News This Week: ICE Can Now Spy on Every Phone in Your Neighborhood' (Wired, 10 January 2026) available at: https://www.wired.com/story/security-news-this-week-ice-can-now-spy-on-every-phone-in-your-neighborhood/.

37 Dell Cameron, 'ICE Wants to Build Out a 24/7 Social Media Surveillance Team' (Wired, 3 October 2025) available at: https://www.wired.com/story/ice-social-media-surveillance-24-7-contract/.

38 Sheera Frankel, Cade Metz, and Julian E. Barnes, 'How Talks Between Anthropic and the Defense Dept. Fell Apart (The New York Times, 1 March 2026) available at: https://www.nytimes.com/2026/03/01/technology/anthropic-defense-dept-openai-talks.html.

data,[39] or on bulk information collected by their intelligence agencies.[40]

The UK similarly moved to make the collection of large amounts of data easier in 2024 when it amended the Investigatory Powers Act to allow for less restrictive access to bulk sets of data deemed to have low or no reasonable expectation of privacy attached to them or held by third parties.[41] This was likely in anticipation of applying AI to the more easily accessible data.[42]

Analysing the Data

The most prominent use of AI by intelligence agencies will likely be for the analysis of the vast amount of data they collect.

Richard Moore, former-chief of MI6, provided several examples of these AI functionalities in his commentary, quoted above, including summarisation, ideation, *"identifying key information in a sea of data"*," 'red teaming'" operations, and using cloud technology for data processing.[43]

Private companies may play a significant role in such analysis, as Moore emphasised the intelligence agencies *"cannot do this alone - our partnership is augmented by a network of partnerships with the private sector."*[44] In 2024, MI6 also published calls for bids from tech companies, one asking for companies that can use AI to *"assist with screening individuals of interest"*,[45] and one asking for AI to support *"human decision making"*.[46] The results of these calls were not published.

39 Faiza Patel, 'AI and the Commercial Data Loophole' (Just Security, 21 July 2026) available at: (https://www.justsecurity.org/148430/ai-surveillance-commercial-data-loophole/.

40 Faiza Patel, AI and Warrantless Foreign Intelligence Surveillance (Just Security, 22 July 2026) available at: https://www.justsecurity.org/148444/ai-warrantless-foreign-intelligence-surveillance/.

41 'PI response to Home Office consultation on codes of practice under the Investigatory Powers (Amendment) Act 2024' (Privacy International, 16 January 2025) available at: https://privacyinternational.org/advocacy/5512/pi-response-home-office-consultation-codes-practice-under-investigatory-powers.

42 Ibid.; see also Harry Davies, 'UK intelligence and spy agencies relax burdensome laws on AI data, says report' (The Guardian, 1 August 2023) available at: https://www.theguardian.com/technology/2023/aug/01/uk-intelligence-spy-agencies-relax-burdensome-laws-ai-data-bpds.

43 B. Burns and R. Moore, Intelligence partnership helps the US and UK stay ahead in an uncertain World (n 26).

44 Ibid.

45 'Use of AI in screening individuals of interest' (IUK Business Connect) available at: https://iuk-business-connect.org.uk/opportunities/use-of-ai-in-screening-individuals-of-interest/, accessed 10 September 2026.

46 'Innovation Exchange Challenge: How can we capture complex human judgement to make better decisions supported by AI?' (IUK Business Connect) available at: https://iuk-business-connect.org.uk/opportunities/innovation-exchange-challenge-how-can-we-capture-complex-human-judgement-to-make-better-decisions-supported-by-ai/, accessed 10 September 2026.

Several UK police forces are reportedly working with Palantir to build a real time surveillance network,[47] which could just as easily be utilised by intelligence agencies. Palantir's software will reportedly be used to *"assist with decision making"*, *"aid in the prevention, detection, and investigation of crimes"*, and create profiles of people, although Palantir denies it software will be used for predictive policing.[48]

In February 2025, the UK's GCHQ published a white paper called 'Pioneering a New National Security: The Ethics of Artificial Intelligence.' In it, it vaguely outlines how GCHQ is using AI to process data, promote online safety, and prevent child trafficking.[49] It does acknowledge that there are issues with AI, including a lack of transparency, fairness, and privacy, but assures readers that it is implementing AI with these issues in mind, and that it has developed an internal AI Ethical Code of Practice and Governance.[50]

These glimpses illustrate how the UK may be utilising AI for intelligence work, including for:

- **Summarisation;**
- **Ideation;**
- **Identifying key information in a 'sea of data';**
- **'Red teaming' operations;**
- **Sentiment analysis;**
- **Detecting relationships;**

47 Mark Wilding and Cahal Milmo, 'UK police working with controversial tech giant Palantir on real-time surveillance network' (Liberty Investigates, 16 June 2025) available at: https://libertyinvestigates.org.uk/articles/uk-police-working-with-controversial-tech-giant-palantir-on-real-time-surveillance-network/.

48 Ibid.

49 'Pioneering a New National Security: The Ethics of Artificial Intelligence' (GCHQ, February 2025) available at: https://www.gchq.gov.uk/artificial-intelligence/index.html, accessed 10 September 2026.

50 Ibid.

- Assisting with decision making; and
- Profiling.

Other countries' AI tools also shed light on what intelligence agencies may be able to do.

China is a keen innovator in aggregating and analysing masses of data, including for intelligence purposes. In China, the government reportedly uses AI-enabled surveillance tools to surveil the Uygher population in Xinjiang province under the guise of counter-terrorism.[51] Authorities have detained Uygher citizens in re-education camps based on the outcomes of ambiguous AI-based analyses.[52] According to the New York Times, China also uses a massive network of AI-enabled facial recognition cameras to facilitate its social credit system by analysing public and private social and behavioural data from financial transactions, health records, and employment status.[53] In 2026, details emerged about how foreign residents in China are monitored, including by collecting and aggregating data from cameras, medical records, bills, and travel.[54]

Investigative journalists have disclosed how Israel's intelligence agencies, including their military intelligence agency, have adopted AI tools. A joint investigation by +972 Magazine, the Guardian, and Local Call, revealed that to process the vast data collected through interception of Palestinian telephone and text communications, the Israeli military intelligence agency trained a large-language model to understand spoken Arabic.[55] One technologist involved in the creation of the system said *"[w]e tried to create the largest dataset*

51 H. Akin ÜNVER, 'Artificial intelligence and human rights: Using AI as a weapon of repression and its impact on human rights' (European Parliament, Directorate-General for External Policies, May 2024) available at:

https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf, pp. 16-19.

52 Ibid.

53 Paul Mozer, 'As China rushes to embrace surveillance tech, citizens risk a chilling future' (The New York Times, 8 July 2018) available at: https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

54 Lily Kuo and Pei-Lin Wu, 'How China Keeps Tabs on Foreigners' (The New York Times, 2 August 2026) available at: https://www.nytimes.com/2026/08/02/world/asia/china-surveillance-foreigners-database.html.

55 Harry Davies and Yuval Abraham, 'Revealed: Israeli Military creating Chat GPT-like tool using vast collection of Palestinian surveillance data' (The Guardian, 6 March 2025), available at: https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.

possible [and] collect all the data the state of Israel has ever had in Arabic."[56]

The processing of so much data may require cloud computing. In 2025, Microsoft abandoned elements of its contract with the Israeli government that provided the military intelligence agency with segregated access to its Azure cloud platform.[57] They did so, according to the Guardian and +972 Magazine, because Israeli authorities were using Azure to process data under the mantra of 'a million calls an hour', capturing everyday Palestinian communications, initially from the West Bank but expanding its collection.[58] Internal files suggest that as of July 2025, Israel stored up to 11,500 terabytes of data, equivalent to approximately 200 million hours of audio, on Microsoft servers in the Netherlands, and that it planned to transfer even more data.[59] AI-facilitated analysis of this data appears to have included a method called 'noisy message' which *"scanned all texts messages between Palestinians in the West Bank and assigned each message a risk rating based on an automated analysis of whether it included words deemed to be suspicious."*[60] During the war in Gaza, the cloud-based system was reportedly *"put to frequent use alongside a series of AI-driven target recommendation tools."*[61]

The Israeli military has reportedly been using a series of AI systems, including one called *"Lavender"* that analyses mass surveillance data to identify *"incriminating features"* and target suspected Hamas militants, at one point flagging up to 37,000 people as targets.[62] Another system called *"The Gospel"* uses "enormous amounts" of surveillance data from a range of sources to generate scores for an *"AI target bank"*, dramatically increasing the number of target recommendations for bombings, or as one former intelligence officer explained, a *"mass assassination*

56 Ibid.

57 Harry Davies and Yuval Abraham, 'Microsoft blocks Israel's use of its technology in mass surveillance of Palestinians' (The Guardian, 25 September 2025) available at: https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.

58 Harry Davies and Yuval Abraham, '"A million calls an hour": Israel relying on Microsoft cloud for expansive surveillance of Palestinians' (The Guardian, 6 August 2025) available at: https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.

59 Ibid.

60 Ibid.

61 Ibid.

62 Yuval Abraham, '"Lavender": The AI machine directing Israel's bombing spree in Gaza' (+972 Magazine, 3 April 2024) available at: https://www.972mag.com/lavender-ai-israeli-army-gaza/.

factory".[63] Additionally, Israel has used AI to listen in on calls, use them to generate an approximate location for the target, then launch airstrikes.[64]

These instances illustrate that intelligence agencies possess vast amounts of data and seek access to more, and that they apply AI tools and make determinations that affect people's lives.

These examples from China and Israel expand our AI use cases to include:

- Surveillance of entire populations of certain ethnicities or minority groups;
- Facilitating social credit systems;
- Monitoring foreigners in country;
- Using LLMs to understand spoken language and analyse audio communications at scale;
- Assigning risk ratings to communications at scale;
- Generating target recommendations; and
- Analysing audio communications to generate location information for targeting

63 Harry Davies, Bethan McKernan. and Dan Sabbagh, '"The Gospel": how Israel uses AI to select bombing targets in Gaza' (The Guardian, 1 December 2023) available at: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets; Y. Abraham, '"Lavender"' (n 63).

64 Sheera Frenkel and Natan Odenheimer, 'Israel's A.I. Experiments in Gaza War Raise Ethical Concerns' (The New York Times, 25 April 2025) available at: https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html.

1.3 WHY IS THE USE OF AI IN INTELLIGENCE CONTEXTS HARMFUL?

The ways that intelligence agencies appear to be using AI can create unique and far-reaching harms. First, the secrecy with which intelligence agencies have adopted AI is harmful in and of itself, because it has robbed the public of meaningful participation in the debate about the risks to human rights that AI-enabled surveillance and intelligence gathering poses.[65] Second, AI allows intelligence agencies to operate at a massive and unprecedented scale because the technology can independently gather and process data without agencies having to dedicate human resources to the endeavour. In other words, AI enables intelligence agencies to gather more data about more people, without sacrificing other capabilities or activities.[66] Third, agencies are likely using AI to analyse the data they gather, and then profile and make predictions about people, groups, and phenomena, without transparency and safeguards to guarantee the reliability of those profiles and predictions. Some AI systems make recommendations or independently act based on this analysis, with limited or no human involvement.[67] Traditional systems of intelligence regulation and oversight appear to be failing to effectively control these new AI-enabled capabilities.

Secrecy: National Security, AI, and State Secrets

Even though the phenomenon of AI being used in surveillance contexts is well documented, we do not know very much about exactly what technology is being used by which intelligence agencies, or how this technology works. Most governments are refusing to explain how they are using AI,

65 Brennan Center for Justice and ACLU, 'Comment Submitted to the Privacy and Civil Liberties Oversight Board Public Forum on Artificial Intelligence in Counterterrorism and Related National Security Programs' (Brennan Center for Justice, 2 July 2024) available at: https://www.brennancenter.org/our-work/research-reports/comment-submitted-privacy-and-civil-liberties-oversight-board-public.

66 J. Stanley, 'Machine Surveillance is Being Super-Charged by Large AI Models' (n 20).

67 Scoop News Group, 'Too much data, too few analysts: How AI offers a "force multiplier" for intelligence analysts' (DefenseScoop, 12 November 2025) available at: https://defensescoop.com/2025/11/12/too-much-data-too-few-analysts-how-ai-offers-a-force-multiplier-for-intelligence-analysts/; The Economist, 'How spy agencies are experimenting with the newest AI models' (n 21).

claiming that sharing this information would endanger national security.

In the UK, intelligence agencies including MI5, MI6, GCHQ, and the National Crimes Institute are exempt from freedom of information act requests (FOIA) – meaning that it is impossible to even ask the agencies to disclose how they are using AI.[68] In the US, even though it is possible to FOIA intelligence agencies, the requests are often ignored,[69] or the files thoroughly redacted on national security grounds.[70] And although the European Union led the way for AI regulation by passing the AI Act that mandates reporting on when AI is used, there is a national security exemption.[71] What we do know about how AI is being used in surveillance contexts is the result of media reports, successful FOIA requests, leaked documents, and very occasional glimpses provided by intelligence agencies. But in general, in the words of the American Civil Liberties Union and the Brennan Center for Justice,

> *"[t]he lack of proactive and meaningful disclosures from the government makes it nearly impossible for the public to understand how AI systems are used in these operations, how these systems make decisions or recommendations, how their outputs influence agency decisions or action, and what safeguards, if any, are in place."*[72]

This lack of transparency is a problem in a democracy because it prevents effective democratic control of intelligence agencies.[73] And in our current environment, where concerns about the potential for AI's impact, its

68 Information Commissioner's Office, 'Public authorities under the Freedom of Information Act' (ICO, 30 September 2022) available at: https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/public-authorities-under-foia/.

69 ACLU, '*ACLU v NSA* – FOIA Lawsuit Seeking Records About the NSA's Use of Artificial Intelligence' (American Civil Liberties Union, 13 May 2024) available at: https://www.aclu.org/cases/aclu-et-al-v-nsa-et-al-foia-lawsuit-seeking-records-about-the-nsas-use-of-artificial-intelligence.

70 Brennan Center for Justice, Comment Submitted to PCLOB (n 66).

71 Statewatch, '"Cop-out": security exemptions in the Artificial Intelligence Act' (Statewatch, 9 April 2025) available at: https://www.statewatch.org/automating-authority-artificial-intelligence-in-european-police-and-border-regimes/.

72 Brennan Center for Justice, Comment Submitted to PCLOB (n 66).

73 David Anderson Q.C., 'A Question of Trust: Report of the Investigatory Powers Review' (UK Government, June 2015) available at: https://assets.publishing.service.gov.uk/media/5a7f9b66ed915d74e622b7ca/IPR-Report-Web-Accessible1.pdf.

use and abuse, are extremely paramount,[74] there is no good reason for the intelligence agencies to be exempt from the discussion.

Surveillance at Scale

In 2012, the US Supreme Court considered how the law should approach the vast quantities of data that technology allows the government to collect about people. In *US v Jones*, the Court considered whether evidence obtained after police placed a GPS tracking device on a car without a warrant was admissible. The Court found that the warrantless GPS evidence could not be used for prosecution, citing concerns about the sheer number of people the police could surveil if they did not have to expend manpower on physically following people around.[75]

The scale of AI surveillance is not only concerning because of the vast amount of data underlying it, but because of the potentially exponential increase in the number of people intelligence agencies are able to surveil.[76] Like in *US v Jones*, where a GPS tracking device reduced the cost of surveillance to the government, the resources required for such mass surveillance as the default tool for investigation has dramatically decreased as a result of: the precipitous decline in the cost of technology and data storage; the ubiquity of digital devices and connectivity; and the exponential increase in the processing power of computers.[77] This environment allows the government to surveil whomever they wish, without having to prioritise legitimate suspects.[78]

In early 2026, Home Secretary Shabana Mahmood appeared to welcome the vast capabilities of AI. She said in an interview with the Telegraph: [79]

> *"When I was in justice, my ultimate vision for that part of the*

74 See, e.g., Independent International Scientific Panel on AI, 'Preliminary Report' (United Nations, July 2026) available at: https://www.un.org/independent-international-scientific-panel-ai/sites/default/files/2026-07/en_Preliminary%20Report_.pdf.

75 *United States v Jones*, 565 US 400 (2012).

76 J. Stanley, 'Machine Surveillance is Being Super-Charged by Large AI Models' (n 20).

77 UN HRC Report A/HRC/52/39 (n 15), para 9.

78 United Nations General Assembly, Report A/69/397, available at: https://docs.un.org/A/69/397, para 19.

79 'Criminals to be stopped by 'Minority Report'-style policing plans using AI' (The Telegraph, 18 January 2026) available at: https://www.telegraph.co.uk/news/2026/01/18/criminals-stopped-minority-report-style-policing-plans-ai/.

criminal justice system was to achieve, by means of AI and technology, what Jeremy Bentham tried to do with his Panopticon. That is that the eyes of the state can be on you at all times."

The Panopticon, theorised by English philosopher Jeremy Bentham, is a design for a prison that features a circular structure with individual cells surrounding a central guard tower.[80] The structure is lit so that guards can observe inmates at all times, but inmates cannot see the guards. Secretary Mahmood's vision is not far off. Thanks to AI's ability to collect and analyse data from so many disparate sources, it can paint an incredibly detailed picture of someone's life – capturing their political beliefs, sexual orientation, relationship status, health issues, political activity, family life, social circle, financial situation, and so much more. Yet the lack of transparency around AI's use by intelligence agencies means they largely remain in the dark like Bentham's guards.

Today, governments have access to vast amounts of personal data that can reveal individuals' location, age, gender, political beliefs, hobbies, sexual orientation, medical conditions, religious beliefs, and who they contact.[81] There are three main ways intelligence agencies access data.



First, as revealed by Edward Snowden in 2013, governments, including the UK's GCHQ, collect bulk telecommunications data and content through methods such as intercepting internet traffic, hacking, recording phone calls, copying address books, and

80 UCL Bentham Project, 'Panopticon' (University College London) available at: https://www.ucl.ac.uk/laws/research/research-projects/bentham-project/about-jeremy-bentham/panopticon, accessed 10 September 2026.

81 Christian Ruckerbauer and Thorsten Wetzling, 'Data bought, rights ignored: European intelligence services' use of commercially sourced data' (Interface, 16 June 2026) available at: https://www.interface-eu.org/publications/governance_of_data_purchases_by_european_intelligence_agencies, p. 7.

more.[82] These programs are far reaching and intrusive, recording where people go, with whom they speak, and their web activity.[83] The UK also likely has access to information intercepted in bulk by the US government, and the other members of the Five Eyes Alliance.[84]

Second, national security agencies work closely with technology companies and data brokers to acquire, access, and use large volumes of personal data held by the private sector.[85] The Interface recently published a report describing this phenomenon, and shows that the sources of this data, and the ways governments come to access it, are varied, but include bidding at auctions, software development kits, social media, exploiting technical vulnerabilities, and applications connected to the Internet of Things.[86] These platforms do not set out to collect this data for governments. Rather, they collect it to enable targeted advertising, product optimization, and enhanced user experiences, then analyse this information to monetize or personalize their services.[87] Intelligence agencies have a number of means of accessing this private data, including through: direct procurement from commercial vendors of datasets generated from data used for advertising or from data leaks;[88] purchasing surveillance or SOCMINT platforms[89] that provide access to aggregated and already processed personal data;[90] and direct collection through the development



82 Privacy International, 'How Bulk Interception Works' (Privacy International, 19 July 2016) available at: https://privacyinternational.org/long-read/827/how-bulk-interception-works; Privacy International, 'Government Hacking' (Privacy International) available at: https://privacyinternational.org/learn/government-hacking, accessed 10 September 2026.

83 Privacy International, How Bulk Interception Works' (n 83).

84 Ibid.

85 C. Ruckerbauer and T. Wetzling, 'Data brought, rights ignored' (n 81), p. 8.

86 Ibid.

87 Ibid.

88 Ibid., p. 9.

89 Ibid.

90 Ibid., p. 8.

of shell companies that engage in the ad tech industry.[91] In addition to analysing this data, intelligence agencies can use this information to train their AI models.[92]



Third, intelligence agencies additionally likely have access to vast amounts of data held on government databases, including driver's license,[93] passport and immigration databases,[94] and law enforcement databases.[95] In the UK, law enforcement agencies are building an even more integrated data platform, the National Data Integration and Exploitation Service (NDIES), that will further combine sources of data that were traditionally siloed.[96] We do not know, but do assume, that intelligence agencies will be able to access NDIES.

Today in the UK, bulk surveillance capabilities are mostly regulated by provisions in the Investigatory Powers Act 2016, and UK intelligence agencies need a warrant before collecting or accessing the desired information. But, as discussed in more detail below, those warrants do not sufficiently protect our privacy considering AI advancements that make it vastly easier to process and analyse this data. Tools

91 Ibid.

92 Ibid.

93 BBC News, 'US judge rules NSA phone surveillance programme was illegal' (BBC News, 9 July 2019) available at: https://www.bbc.co.uk/news/world-us-canada-48907026; Katy Watts, 'Surveillance Britain: where police are quietly trying to access 50m photos for one mass lineup' (The Guardian, 21 December 2023) available at: https://www.theguardian.com/commentisfree/2023/dec/21/surveillance-britain-police-photos-facial-recognition.

94 Privacy International, 'Revealed: "Skyrocketing" scale of UK police's Secret Facial Recognition Searches of Passport and Immigration Databases' (Privacy International, 7 August 2025) available at: https://privacyinternational.org/news-analysis/5635/revealed-skyrocketing-scale-uk-polices-secret-facial-recognition-searches/.

95 Home Office, 'Law Enforcement Data Service (LEDS): data protection impact assessment (accessible)' (GOV.UK, 24 June 2026) available at: https://www.gov.uk/government/publications/law-enforcement-data-service-data-protection-impact-assessment-2026/law-enforcement-data-service-leds-data-protection-impact-assessment-accessible.

96 National Police Chiefs' Council, 'Bridging the gap between force data' (NPCC News, 29 January 2026) available at: https://news.npcc.police.uk/releases/bridging-the-gap-between-force-data-to-ensure-policing-can-better-join-the-dots.

like Palantir's[97] Investigative Case Management system, used by the US's ICE, can help governments manage these vast quantities of data from all of these sources by combining them into a single investigative platform that lets agents search using categories like immigration status, scars, tattoos, and license plate number.[98] Examples discussed above, particularly coming out of Israel, demonstrate the vast power of modern processing which can identify tens of thousands of potential targets from bulk data.[99] By combining government datasets with commercial datasets, and using AI to analyse it all, intelligence agencies are likely able to create full pictures of individuals lives that would otherwise be impossible.

97 Palantir is also operating similar software in the United Kingdom, including with Bedfordshire police, M. Wilding and C. Milmo, 'UK police working with controversial tech giant Palantir on real-time surveillance network' (n 48).

98 Caroline Haskins, 'ICE Is Paying Palantir $30 Million to Build 'ImmigrationOS' Surveillance Platform' (WIRED, 18 April 2025) available at: https://www.wired.com/story/ice-palantir-immigrationos/.

99 See, e.g., Y. Abraham, '"Lavender"' (n 63).

Making sense of it all



Before AI, thousands of people would have had to comb through this data, in a post-9/11 framing, needles in illicitly gathered haystacks. AI makes this easier – based on the data it is fed, algorithms can paint a picture of what someone's life looks like – where do they work? What are their habits? Who is their family? What do they believe? What is their immigration status? It can also figure out vital information like relationships between individuals and between groups, how movements are funded, and where crime may potentially occur. It can infer characteristics from disparate pieces of information. And all this information can now likely be accessed with natural language queries, similar to those we are becoming used to employing with commercially available AI tools.

This power is dangerous, and it is not clear whether governments are wielding it responsibly. The onset of governments' power to surveil virtually every aspect of every person's life has coincided with a marked shift towards authoritarianism, and a turn away from respect for international human rights.[100] While using surveillance to effectuate authoritarianism is nothing new, the difference in a post-AI world is the scale at which governments can act. Below we highlight some of our most pressing concerns with the scaled-up potential for intelligence analysis: problematic prediction; AI-generated errors and bias; and opaque reasoning.

These examples are far from exhaustive but illustrate the kinds of human rights concerns enabled by AI – each scenario required data collection, data analysis, surveillance, and tracking of thousands of individuals. Without AI, these activities would, at best, take vast amounts of manpower and would likely be impossible.

100 UN HRC Report A/HRC/52/39 (n 15), para 9.; H. ÜNVER, 'AI and Human Rights' (n 52).

Predictive "Intelligence"

Government agencies increasingly rely on AI systems to make predictions about human behaviour and to make decisions or recommendations about how the state should treat these people. AI tools can make decisions about whether a person should be surveilled, detained, or interrogated;[101] whether they should be allowed to access rehabilitative services or welfare payments;[102] whether they should or should not be granted immigration status;[103] and even whether they should be killed or be allowed to live.[104] In these contexts, AI risks violating the most fundamental of human rights, and realistically, they represent only a handful of use cases for intelligence agencies.

Both US and UK intelligence officials have confirmed that predictive AI is being used in intelligence agencies to some degree[105] – while we cannot analyse the risks of actual use-cases, predictive AI in intelligence and law enforcement contexts opens the door to several types of potential harms. *"Evidence-based assessment tools,"* or risk assessments *"try to predict recidivism — repeat offending or breaking the rules of probation or parole — using statistical probabilities based on factors such as age, employment history and prior criminal record."*[106] Today, law enforcement bodies across the UK reportedly use risk assessment tools to make decisions at all stages of the criminal justice process.[107]

101 Electronic Privacy Information Center, 'AI in Law Enforcement' (EPIC) available at: https://epic.org/issues/ai/ai-in-the-criminal-justice-system/, accessed 10 September 2026.

102 Statewatch, 'New Technology, Old Injustice: Data-driven discrimination and profiling in police and prisons in Europe' (Statewatch, 30 June 2025) available at: https://www.statewatch.org/publications/reports-and-books/new-technology-old-injustice-data-driven-discrimination-and-profiling-in-police-and-prisons-in-europe/.

103 Robert Booth, 'AI tool could influence Home Office immigration decisions, critics say' (The Guardian, 11 November 2024) https://www.theguardian.com/uk-news/2024/nov/11/ai-tool-could-influence-home-office-immigration-decisions-critics-say.

104 Nilza Amaral, 'The Iran war highlights the creeping use of AI in warfare' (Chatham House, 27 March 2026) available at: https://www.chathamhouse.org/2026/03/iran-war-highlights-creeping-use-ai-warfare; Elke Schwarz, 'Gaza war: Israel using AI to identify human targets raising fears that innocents are being caught in the net' (Queen Mary University of London, 17 April 2024) available at: https://www.qmul.ac.uk/media/news/2024/hss/gaza-war-israel-using-ai-to-identify-human-targets-raising-fears-that-innocents-are-being-caught-in-the-net.html.

105 B. Burns and R. Moore, Intelligence partnership helps the US and UK stay ahead in an uncertain World (n 26).

106 Electronic Privacy Information Center, '*EPIC v DOJ* (Criminal Justice Algorithms)' (EPIC) available at: https://epic.org/documents/epic-v-doj-criminal-justice-algorithms/, accessed 10 September 2026.

107 Oxford Institute of Technology and Justice, 'United Kingdom: A form of AI at every stage of the criminal process' (Oxford Institute of Technology and Justice, June 2026) available at: https://www.techandjustice.bsg.ox.ac.uk/research/united-kingdom.

These predictive AI tools suffer from two fundamental flaws: (1) a significant potential for error, inaccuracy or bias to creep into the assessment, which is (2) compounded by the opaque nature of the reasoning underlying such predictions. We discuss both below.

The prevalence of errors and bias

AI is not flawless. It may recreate and amplify human bias, hallucinate or otherwise be unreliable, making it even more dangerous to our rights.

Numerous studies looking at the use of predictive AI tools in policing have shown that when software is trained on previous law enforcement data, and that data contains biases, such as discrimination against certain communities, the system might also learn to propagate those biases.[108] For example, a 2026 study commissioned by the Mayor of London found that black Londoners are up to 48 times more likely to be stopped and searched by police.[109] If we train systems on that data, we risk propagating those biases and discriminatory activity.

In the US, multiple lawsuits have been brought against police departments for their use of predictive policing software. [110] In Pasco County, Florida, the Sherriff admitted after lengthy litigation that he had been using an unconstitutional predictive policing program that used an algorithm to produce a list of *"prolific offenders."*[111] Although the kinds of data this algorithm analysed were never fully revealed; race, ethnicity, social-economic status, and whether or not

108 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing' (Amnesty International UK, 1 February 2025) available at: https://www.amnesty.org.uk/knowledge-hub/all-resources/automated-racism-report/; Matthew Browning and Bruce Arrigo, 'Stop and Risk: Policing, Data, and the Digital Age of Discrimination' (American Journal of Criminal Justice, 46, 298–31 (2021)) available at: https://doi.org/10.1007/s12103-020-09557-x; Eylül Bozkır, Yueqi Chen, Sarah Ghulam, Qixun Ma, Raha Razmi, Rhea Swaminathan and Iniya Thiru, 'Predictive Policing or Predictive Prejudice? A Study of the Legal, Historical and Ethical Implications of AI in Policing' (OxJournal, 18 August 2025) available at: https://www.oxjournal.org/predictive-policing-or-predictive-prejudice/.

109 Mayor of London, 'Largest-ever research project on police use of Stop and Search highlights how significant disproportionality in London can be addressed' (London City Hall, 10 March 2026) available at: https://www.london.gov.uk/largest-ever-research-project-police-use-stop-and-search-highlights-how-significant-disproportionality-in-london-can-be-addressed.

110 *EPIC v DOJ* (n 107); Dave Collins, 'Police departments sued over predictive policing programs' (Police1, 5 July 2018) available at: https://www.police1.com/legal/articles/police-departments-sued-over-predictive-policing-programs-oEOyziTEEgyMrLNv/.

111 J. Justin Wilson, 'Case Closed: Pasco Sheriff Admits "Predictive Policing" Program Violated Constitution' (Institute for Justice, 4 December 2024) available at: https://ij.org/press-release/case-closed-pasco-sheriff-admits-predictive-policing-program-violated-constitution/.

a family member had previously committed a crime were factors, and the community reported that black individuals were disproportionately affected by the program.[112] Based solely on their inclusion on this list, and not due to other criminal activity, children were targeted and interrogated without supervision, individuals and families were continuously harassed, and the police carried out *"prolific offender checks,"* during which deputies looked to cite the people targeted for issues like having grass that was too long, missing house numbers, unvaccinated pets, and excessive window tint on parked cars.[113]

In Plainfield, New Jersey, police had been using predictive software from Geolitica (formerly PredPol).[114] WIRED conducted a study on the software and found that it was accurate less than 1% percent of the time in predicting where and when crimes were most likely to occur.[115] Additionally, a study from The Markup found that *"the software disproportionately directed officers to patrol neighbourhoods with relatively higher percentages of low-income, Black, and Latino residents compared to those cities or counties on the whole"*.[116] The Plainfield Police Captain later admitted the police force rarely used the predictive software.[117]

Another form of error is when AI systems hallucinate.[118] The tools may draw false or misleading conclusions in their analysis of context and data. They may even fabricate data and present it as factual.[119] This is why it is so important for reasoning and decisions to be checked. If given vast amounts of personal data, say an entire social media history of numerous people, the conclusions drawn may not be accurate or reliable.

112 Ibid.

113 Ibid.

114 Dhruv Mehrotra and Annie Gilbertson, 'Predictive Policing Software Terrible at Predicting Crimes' (WIRED, 2 October 2023) available at: https://www.wired.com/story/plainfield-geolitica-crime-predictions.

115 Ibid.

116 Aaron Sankin and Surya Mattu, 'How We Assessed the Accuracy of Predictive Policing Software' (The Markup, 2 October 2023) available at: https://themarkup.org/show-your-work/2023/10/02/how-we-assessed-the-accuracy-of-predictive-policing-software.

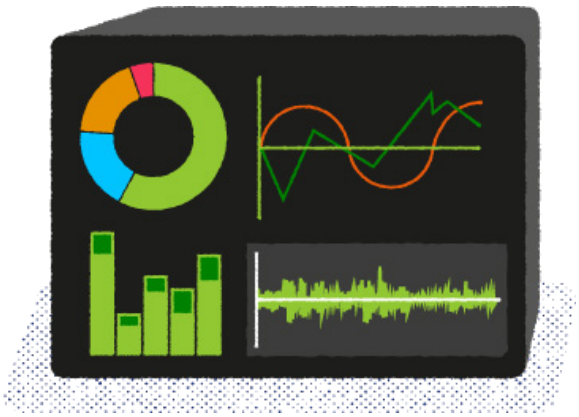
117 D. Mehorta and A. Gilbertson, 'Predictive Policing Software Terrible at Predicting Crimes' (n 114).

118 United Nations Independent International Scientific Panel on Artificial Intelligence, 'Preliminary Report' (United Nations, July 2026) available at: https://www.un.org/independent-international-scientific-panel-ai/sites/default/files/2026-07/en_Preliminary%20Report_.pdf, pp.12, 15, 28-30.

119 See, e.g., HAQQ Team, 'AI Hallucination Cases: The 1,598-Case Sanctions Tracker' (HAQQ, 22 May 2026; updated 11 June 2026) available at: https://www.haqq.ai/blog/ai-legal-hallucination-audit.

This was part of the conflict between Anthropic and the Department of Defense in early 2026. On top of the privacy concerns of building comprehensive pictures of people's lives automatically and at massive scale, Anthropic also said that *"frontier AI systems are simply not reliable enough to power fully autonomous weapons."*[120]

The fact that predictive policing software, manufactured by some of the same companies likely providing AI-enabled surveillance tools to intelligence agencies, is simply bad at its job has not stopped its proliferation. Although we do not know how intelligence agencies are using AI to make predictions, we strongly suspect that they are doing so, and we also know that intelligence agencies are not immune to discrimination,[121] likely meaning that the datasets with which they train predictive AI models may be similarly tinged with bias and inaccuracy.



Opaque Reasoning

In general, in the UK, law enforcement and intelligence agencies must have a reason to place an individual under surveillance, or take other action against them, such as arrest.[122] For example, in law enforcement contexts, authorities must have *"reasonable grounds to suspect"* that someone has committed or will commit a crime before arresting them.[123] Likewise, in intelligence contexts, when deciding whether to place someone under surveillance, an officer must first seek approval from a higher authority, or even the Home Office

120 Anthropic, 'Statement on the comments from Secretary of War Pete Hegseth' (Anthropic, 27 February 2026) available at: https://www.anthropic.com/news/statement-department-of-war.

121 Faiza Patel, 'The Costs of 9/11's Suspicionless Surveillance: Suppressing Communities of Color and Political Dissent' (Brennan Center for Justice, September 8, 2021) available at: https://www.brennancenter.org/our-work/analysis-opinion/costs-911s-suspicionless-surveillance-suppressing-communities-color-and.

122 'Surveillance law explainer' (Liberty) available at: https://www.libertyhumanrights.org.uk/advice_information/i-think-im-under-surveillance/, accessed 10 September 2026.

123 'Stop and search' (Liberty) available at:

https://www.libertyhumanrights.org.uk/advice_information/stop-and-search/, accessed 10 September 2026.

and a Judicial Commissioner, depending on the type of surveillance.[124]

As intelligence agencies begin to rely on AI to make predictions and decisions about people, it is unclear whether the same standard of proof can be met. When an AI system *"predicts"* that someone is likely to commit a crime and decides or recommends that someone be placed under surveillance, arrested, or targeted in a conflict setting, the AI cannot necessarily articulate the reason why it came to its decision, and as a result humans cannot judge if the AI reached the requisite standard of proof for the action taken.

This is in part because certain AI systems, including the currently most advanced models, are trained on vast amounts of data to produce desired outputs, but how it produces those outputs is often unknown, even to the system's creators.[125] This is often referred to as the *"black box"* problem with AI.[126] Reasons for delivering a particular response may be hard to explain or non-existent, at least in way humans usually understand and articulate *"reasons"*. However, this 'how' is critical to understanding the ways that different AI systems work, what biases they might carry, and their capability to analyse information and make predictions.[127]

This opaque nature of AI decision making also risks individuals' right to a meaningful remedy after the State has taken action – if the government cannot or will not tell individuals why they were targeted, individuals cannot challenge unlawful surveillance or arrest.[128] These risks would exist even if predictive AI was flawless - but unfortunately, as discussed above, it is error-prone and can recreate human bias.

The threats predictive AI poses to due process rights, and the right to a remedy,

124 'Surveillance law explainer' (Liberty) available at:
https://www.libertyhumanrights.org.uk/advice_information/i-think-im-under-surveillance/, accessed 10 September 2026.

125 Matthew Kosinski, 'What is black box AI?' (IBM Think, October 29, 2024) available at: https://www.ibm.com/think/topics/black-box-ai.

126 Lou Blouin, 'AI's mysterious 'black box' problem, explained' (University of Michigan-Dearborn, March 6, 2023) available at: https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained.

127 E. Bozkır et al, 'Predictive policing or predictive prejudice?' (n 109).

128 R. Waldman and I. Dyson, 'The dangers of unregulated AI policing' (n 22); Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (Harvard Journal of Law & Technology, Spring 2018) available at: https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf.

are further reinforced by the national security exemptions that governments use to justify its use. The national security exemptions create a loop: governments use AI in intelligence contexts for national security; the AI recommends someone is targeted; the individual inquires why they were targeted; the government refuses to explain why, because doing so would require disclosing what AI systems are being used and what data these systems were trained on, and sharing details about the AI is deemed contrary to national security.[129] The individual is left in the dark.

In summary, in the best-case scenario, even when governments are acting in good faith, the way that intelligence agencies may be using AI is problematic. Governments are collecting and analysing data about all of us from public and private sources at unprecedented scales and rely on opaque technology to analyse it. Swaths more people risk being unlawfully and unjustly targeted based purely on the recommendation or decision of software that cannot explain its decision-making process, cannot be easily challenged, and may be inaccurate or biased. And all of this is happening behind doors that must remain closed, we are told, for our own safety.

129 Rachel Levinson-Waldman and José Guillermo Gutiérrez, 'DHS Must Overhaul Its Flawed Automated Systems' (Brennan Center for Justice, October 24, 2023) available at: https://www.brennancenter.org/our-work/analysis-opinion/dhs-must-overhaul-its-flawed-automated-systems.

2. HOW IS AI USE BY INTELLIGENCE AGENCIES REGULATED IN THE UNITED KINGDOM?

2.1 INTRODUCTION

This section unpacks the legal framework that regulates the use of AI by intelligence agencies in the UK. In doing so it 1) provides a general overview of the regulatory framework; 2) considers the specifics of data protection law, human rights and equality laws, and intelligence laws. In considering these different areas of laws, it 3) notes significant gaps and highlights concerns where AI use undermines existing safeguards.

General Overview

The UK does not have one singular comprehensive law that regulates the use of artificial intelligence. Instead, it has taken a fragmented, cross-sectoral approach where existing laws are used to govern different aspects of the AI pipeline.[130] The idea is not to regulate the technology itself, but instead to focus on how it's used in specific contexts.[131] This approach is reflected in a 2023 White Paper on AI Regulation, which prioritises innovation.[132] It sets out a framework that is underpinned by 5 principles: 1) safety, security and robustness; 2) appropriate transparency and explainability; 3) fairness; 4) accountability and governance and 5) contestability and redress.[133] With regards to the implementation of these, the White Paper notes:[134]

> *"We will not put these principles on a statutory footing initially. New rigid and onerous legislative requirements on businesses could hold back AI innovation and reduce our ability to respond*

130 Brendan McGurk KC and Joe Tomlinson, 'Artificial Intelligence and Public Law' (Bloomsbury Publishing, 2025) p. 54.

131 UK Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation: government response' (GOV.UK, February 6, 2024) available at: https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response#executive-summary, para 63.

132 UK Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation' (GOV.UK, March 29, 2023; updated August 3, 2023) https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.

133 Ibid., para 10.

134 Ibid.

> *quickly and in a proportionate way to future technological advances. Instead, the principles will be issued on a non-statutory basis and implemented by existing regulators. This approach makes use of regulators' domain-specific expertise to tailor the implementation of the principles to the specific context in which AI is used."*

Of course, not turning these principles into law also means that they don't create legal obligations, or incur penalties for non-compliance.

Despite the fragmented approach, there has been some legislative push for an AI law. A private members bill, the Artificial intelligence (Regulation) Bill (the Bill), was introduced by Lord Holmes in November 2023.[135] It was dropped due to the general election but re-introduced in March 2025.[136] It proposes the establishment of an AI authority, prescribes certain principles, encourages regulatory sandboxes and proposes that AI developers must have a designated AI officer, amongst other things.[137]

Whether the Bill will pass, or even effectively regulate AI is unclear. Until then, the current fragmented approach consists of a mix of voluntary measures and existing laws. The voluntary measures include unenforceable commitments from AI companies,[138] codes of practice, for example the Code of Practice for the Cyber Security of AI,[139] and measures such as the Algorithmic Transparency Recording Standard (ATRS).[140] The ATRS provides a standardised way for the

135 Lord Chris Holmes of Richmond, 'Artificial Intelligence (Regulation) Bill' (Lord Chris Holmes, March 4, 2025), available at: https://lordchrisholmes.com/artificial-intelligence-regulation-bill/.

136 See, Lord Holmes of Richmond, 'Artificial Intelligence (Regulation) Bill [HL]' (UK Parliament, March 4, 2025), available at: https://bills.parliament.uk/bills/3942.

137 See ibid., § 1 – 4.

138 See UK Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation (n 132) para 63.

139 UK Department for Science, Innovation and Technology, 'Code of Practice for the Cyber Security of AI' (GOV.UK, 31 January 2025), available at: https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice/code-of-practice-for-the-cyber-security-of-ai.

140 For more om the ATRS see additionally Government Digital Service, 'Algorithmic Transparency Recording Standard Hub' (GOV.UK, 5 January 2023; updated 8 May 2025), available at: https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub.

public sector to publish information in a repository[141] about the algorithmic tools they use and why.[142] The ATRS is currently only mandatory for central government, but there are plans to broaden this in the future.[143] Notably, there are exemptions which permit non-publication of information.[144] These largely mirror exemptions included in the Freedom of Information Act 2000 and cover things like intellectual property, commercially sensitive information and risks to national security.[145] To date, there have only been 125 records published.[146] Nothing has been published by intelligence agencies, despite the Home Office and Ministry of Defence falling under the initial rollout.[147]

There is also somewhat of a centralised function like an AI authority which is currently undertaken by the Digital Regulation Co-operation Forum (DRCF).[148] We say 'somewhat' because it's a voluntary forum of regulators responsible for digital regulation. It is not a standalone AI Regulator[149] as we understand them in other sectors such as the Information Commissioner's Office (ICO) for data protection. It currently includes the Competition and Markets Authority, the Financial Conduct Authority, the Information Commissioner's Office and Ofcom.[150] Legal scholars, Brendan McGurk, KC, and Professor Joe Tomlinson, authors of the authoritative text Artificial Intelligence and Public Law, have notably remarked

141 See the repository of published ATRS records. Cabinet Office, Department for Science, Innovation and Technology and Government Digital Service, 'Find out how algorithmic tools are used in public organisations' (GOV.UK), available at: https://www.gov.uk/algorithmic-transparency-records.

142 Government Digital Service, 'Algorithmic Transparency Recording Standard - guidance for public sector bodies' (GOV.UK, 8 May 2025), available at: https://www.gov.uk/government/publications/guidance-for-organisations-using-the-algorithmic-transparency-recording-standard/algorithmic-transparency-recording-standard-guidance-for-public-sector-bodies.

143 Government Digital Service, 'Algorithmic Transparency Recording Standard (ATRS) Mandatory Scope and Exemptions Policy' (GOV.UK, 17 December 2024), available at: https://www.gov.uk/government/publications/algorithmic-transparency-recording-standard-mandatory-scope-and-exemptions-policy/algorithmic-transparency-recording-standard-atrs-mandatory-scope-and-exemptions-policy.

144 Ibid.

145 Ibid.

146 As of 29 March 2026. To access, see n 143.

147 Government Digital Service 'Policy Paper: Algorithmic Transparency Recording Standard (ATRS) Mandatory Scope and Exemptions Policy' (n 144).

148 Digital Regulation Cooperation Forum, 'Terms of Reference' (GOV.UK, 5 September 2022), available at: https://www.gov.uk/government/publications/drcf-terms-of-reference/terms-of-reference.

149 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 54.

150 See additionally Digital Regulation Cooperation Forum, 'Digital Regulation Cooperation Forum' (DRCF) available at: https://www.drcf.org.uk/.

on the fact that the Equality and Human Rights Commission is not a member.[151]

Some of the existing laws that regulate elements of AI in the UK include data protection law, financial services law, competition law, communications law and equality and human rights law.[152] For intelligence agencies, it also includes sector specific laws such as the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000.

Each of these laws regulate different elements of the AI pipeline. To understand the regulation, we have broken down the chain of activities, or AI pipeline, into three distinct stages:

- **Stage 1: data collection;**
- **Stage 2: making the data useable; and**
- **Stage 3: using the data**
    - **3.1 for training**
    - **3.2 for analysis for operational purposes.**

These different stages and the basics of how they are regulated are depicted in the table and infographic attached as appendices 1 and 2. Stage 3 'using the data' includes two sub-categories which describe how the data may be used. Either to train models (3.1) and/or analysed for operational purposes (3.2). This is because once data is collected, these appear to be its typical use cases, both within intelligence agencies and outside.[153] We assume that intelligence agencies are using data to train models, because it was reportedly the reason they lobbied

151 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 57.

152 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 60.

153 Department for Science, Innovation & Technology, Office for Artificial Intelligence and Centre for Data Ethics and Innovation, 'A Guide to Using Artificial Intelligence in the Public Sector' (GOV.UK, 10 June 2019), available at: https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector.

the government to relax surveillance laws.[154] Stage 3.2 'analysis for operational purposes' looks at some of the operational reasons intelligence agencies may be using AI, such as facial recognition, sentiment analysis or predictive mapping.

These use cases are largely based off the examples we found in section 1 (and as included in the table in appendix 1), and some are assumptions based on existing capabilities of commercially available AI. Our analysis does not focus on any internal ways that agencies may be using AI, for example, to summarise or develop briefing notes or meeting minutes.

154 H. Davies, 'UK Spy Agencies Want to Relax 'Burdensome' Laws on AI data use' (n 42).

2.2 UNDERSTANDING THE REGULATION

In this section we focus on three areas of law:

- **Data protection;**
- **Human rights and equality laws; and**
- **Some of the relevant laws that regulate intelligence services.**

We briefly consider how these laws apply to AI in general and discuss notable considerations in their application to intelligence agencies. In general, although these three areas of law do apply to intelligence agencies use of AI, broad national security exemptions enable non-compliance with them. Additionally, the nature of AI systems, and particularly, their ability to *"learn"* and retain information, means that existing regulation is simply insufficient, and existing safeguards are undermined.

Data Protection Law

Data Protection Law is doing a lot of the heavy lifting in the regulation of AI. In the UK, this consists of the United Kingdom General Data Protection Regulation (UK GDPR)[155] and the Data Protection Act 2018 (DPA).[156] As noted by legal experts, McGurk and Tomlinson *"[a]bsent a more comprehensive regulatory regime specifically for AI, the UK GDPR and the DPA 2018 are the most relevant UK legislation that applies to the deployment of AI systems in the UK."*[157] This makes sense in light of the relationship between AI and data – they need each other. The development of machine learning algorithms requires enormous amounts of data to train models to spot patterns, make predictions, learn and improve.[158] In turn, AI

155 European Parliament and Council of the European Union, 'Regulation (EU) 2016/679 (General Data Protection Regulation)' (EUR-Lex, 27 April 2016), available at: https://www.legislation.gov.uk/eur/2016/679/contents.

156 Data protection Act 2018 (DPA), available at: https://www.legislation.gov.uk/ukpga/2018/12/contents.

157 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 60.

158 Joe McKendrick, 'The Data Paradox: Artificial Intelligence Needs Data, Data Needs AI' (Forbes, 27 June 2021), available at: https://www.forbes.com/sites/joemckendrick/2021/06/27/the-data-paradox-artificial-intelligence-needs-data-data-needs-ai/.

tools help collect the data, prepare it for analysis and analyse large volumes of it.[159]

Where AI uses or processes personal data – in training, testing or analysis – it could fall within the scope of data protection laws and thus need to comply with them.[160] This applies to private and public bodies[161] – including intelligence services. Data protection law can accordingly apply to each of the three stages of the AI pipeline as evidenced in the table and infographic attached as appendices 1 and 2. As noted by the Information Commissioner's Office and the Alan Turing Institute, a research institute founded and funded by the UK government:[162]

> *"[v]ery often, AI does use or create personal data. In some cases, vast amounts of personal data are used to train and test AI models. On deployment, more personal data is collected and fed through the model to make decisions about individuals. Those decisions about individuals – even if they are only prediction or inferences – are themselves personal data."*

And during each of these stages, such processing will need to comply with the principles, requirements and rights included in the law.[163] This is required even when public bodies use systems developed by private bodies. As noted by McGurk and Tomlinson:[164]

> *"A public authority that procures, from a private provider, an AI system to be deployed in support of the provision of public services or public decision-making, remains responsible for the systems compliance with data protection law even though it was not the developer of the system. The nature and extent of its obligations will depend on whether*

159 Ibid.

160 Information Commissioner's Office and The Alan Turing Institute, 'Explaining Decisions Made with AI' (Information Commissioner's Office, 17 October 2022), available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/.

161 UK GDPR art. 4(7-8); see additionally, B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 59-77 for a further discussion of data protection law.

162 ICO 'Explaining Decisions made with AI' (n 161) p. 19.

163 A comprehensive discussion of these obligations in the context of AI is beyond the scope of this paper. See additionally, Information Commissioner's Office, 'Guidance on AI and data protection' (Information Commissioner's Office, 15 March 2023), available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

164 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153).

the contractual arrangements and division of responsibilities with the AI supplier render it a processor, a controller or a joint controller."

Data protection law accordingly places important safeguards on AI's use of personal data. It does so through the seven key principles: lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy, storage limitation; integrity and confidentiality and accountability.[165] However, it is important to note here, that some of the inherent characteristics of AI challenge our conceptions of these classic data protection principles – for example, the sheer volume of data required to train AI seems at odds with the principle of data minimisation.[166]

Data protection law also provides safeguards through the provision of certain rights[167] the most important of which, in the context of AI, includes the right against automated decision making.[168] The right places certain restrictions on automated decision-making, and requires that where significant decisions are taken about a data subject that are based *"entirely or partly on personal data, and based solely on automated processing, the controller must ensure that safeguards for the data subject's rights, freedoms and legitimate interests are in place."*[169] The safeguards must include measures which: a) provide the data subject with information about such decisions; b) enable the data subject to make representations; c) enable the data subject to obtain human intervention and d) enable the data subject to contest decisions.[170]

The application of data protection laws to intelligence agencies

Although data protection laws do a lot of the regulatory heavy lifting, they don't always effectively regulate personal data processing by intelligence services. This is predominantly because of built in broad

165 UK GDPR, art. 5(1)(a) – (f); See additionally: ICO guidance on AI and data protection (n164).

166 See additionally Tara Davis and Wendy Trott, 'The regulation of artificial intelligence through data protection laws: Insights from South Africa' (African Journal on Privacy & Data Protection, 2024), available at: https://ajpdp.unilag.edu.ng/index.php/davis-t-trott-w; see also Privacy International, 'PI response to ICO consultation on web scraping by generative AI' (Privacy International, 5 March 2024), available at: https://privacyinternational.org/advocacy/5263/pi-response-ico-consultation-web-scraping-generative-ai.

167 UK GDPR, Chapter III, arts 12 – 23.

168 UK GDPR, arts 22A – 22D.

169 UK GDPR, art. 22C(1).

170 UK GDPR, art. 22C(3).

exemptions which enable non-compliance with the law.

Intelligence services (including the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ)[171]) are not subject to the whole of the UK GDPR[172] or the law enforcement provisions of the DPA.[173] Instead, they are only subject to Part 4 of the DPA.[174]

At first glance, Part 4 of the DPA seems to provide most of the bells and whistles we'd hope to see. The data protection principles are there,[175] and so are the data subject rights[176] including the rights related to automated processing[177] and information about decision making.[178] Although notably, the safeguards required in relation to automated decision-making, discussed above, are not required under Part 4 of the DPA.

There are two main points to highlight concerning the application of Part 4 of the DPA: 1) the broad exemption for national security; and 2) the gap concerning notification of security breaches.



The national security exemption

Despite Part 4 of the DPA including the typical data protection safeguards, most of them can be largely ignored by the intelligence services. This is permitted through a broad exemption for national security provided in section 110.[179] Section 110 permits non-compliance with certain provisions *"if exemption from the provision is required for the purpose of safeguarding national security."*

Section 110 enables non-compliance with a list of

171 Data Protection Act 2018, Part 4, art. 82(2).

172 European Union, 'Regulation (EU) 2016/679 (General Data Protection Regulation).

173 Information Commissioner's Office, 'Guide to Intelligence Services Processing' (Information Commissioner's Office) available at: https://ico.org.uk/for-organisations/intelligence-services-processing/.

174 UK GDPR art. 2(2)(c): "this regulation does not apply to the processing of personal data to which Part 4 of the 2018 Act (intelligence services processing) applies."

175 DPA §85(1)(a) – (f).

176 DPA §92(1)(a) – (f).

177 DPA §96-97.

178 DPA §98.

179 DPA §110(1) and (2).

provisions which include: the data protection principles (except the requirement relating to lawfulness of processing);[180] data subject rights[181] and the obligations concerning the communication of a personal data breach to the Commissioner.[182]

Notably, the exemption even limits some of the powers of the Information Commissioner including its power to inspect, operate and test equipment used for the processing of personal data;[183] its obligation to monitor and enforce Part 4;[184] to provide information to a data subject concerning the exercise of their rights;[185] and to conduct investigations on the application of Part 4. The national security exemption can even be used to limit the Commissioner's enforcement provisions such as their notices and powers of entry and inspection,[186] and some offences relating to personal data[187] specifically, those concerning unlawfully obtaining data, and re-identifying de-identified data.[188] These are notable exemptions – the Information Commissioner's Office (ICO) is the independent regulator responsible for enforcing compliance with data protection laws. Restricting the ICO's powers on national security grounds undermines independent oversight and accountability which ultimately impacts public trust.

Importantly, it is not clear how it is determined that an exemption is actually required for the purposes of national security. National security is not defined anywhere in the DPA. Further, the law does not specify the factors to consider when making such a determination or even specify the process – including who within the intelligence services makes such a determination, or whether that decision receives third-party authorisation or approval. Section 111 of the DPA provides for a national security certificate which certifies the exemption and serves as conclusive evidence that the exemption from all or any provisions was

180 DPA §110(2)(a).

181 DPA §110(2)(b).

182 DPA §110(2)(c).

183 DPA §119.

184 DPA §110(2)(d)(ii).

185 DPA §110(2)(e)(i) read with Schedule 15.

186 DPA §110(2)(e)(i).

187 DPA §110(2)(e)(i)i.

188 DPA §170 – 173.

required for safeguarding national security.[189] The certificate must be signed by a Minister. But the law doesn't require that a certificate be obtained before applying the exemption. In fact, the Home Office has explicitly confirmed that *"a certificate is not required in order to rely on the national security exemption; in fact, in most cases controllers will determine for themselves whether the national security exemption is applicable."*[190] These certificates can also be pre-emptive and retrospective[191] and can apply for up to 5 years.[192]

A Guidance issued by the Home Office about the national security certificates doesn't shed much additional light on when an exemption would be appropriate. There is one paragraph on it which states:[193]

> *"The controller should assess whether the processing undertaken requires exemption from provisions of the data protection legislation, such as limitations on the data subject's rights, in order to safeguard/protect national security. Any limitations must be proportionate and necessary."*

It doesn't provide any additional clarity on the scope and bounds of what actions or circumstances amount to safeguarding national security.

The ICO has attempted to shed some light on this through a Guidance on the national security exemption.[194] However it refers to the exemption to the extent that it applies to law enforcement in terms of part 3 of the DPA, and not the intelligences services through part 4. That exemption is still overly broad but may be comparatively helpful. It provides:[195]

> *"National security is not specifically defined and can be interpreted in a*

189 DPA §111.

190 UK Government, 'Data Protection Act 2018: National Security Certificates Guidance' (GOV.UK, 19 August 2020), available at: https://assets.publishing.service.gov.uk/media/5f3cfc49d3bf7f1b10d5906d/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.

191 Ibid., p. 4.

192 Ibid., p. 7.

193 Ibid., p. 6.

194 Information Commissioner's Office, 'Guide to Law Enforcement Processing: National Security Exemption', (GOV.UK, 4 November 2025) available at: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

195 Ibid.

flexible way to adapt to changing threats. It is generally understood to cover the security and well-being of the UK as a whole, its population, and its institutions and system of government. For example, it can cover:

- *protection against specific threats, such as from terrorists or hostile states;*
- *protection of potential targets even in the absence of specific threats; and*
- *international co-operation with other countries."*

The effect of this exemption is that intelligence services are permitted, under the broad and undefined purpose of national security, to not comply with most of the data protection safeguards provided by Part 4 of the DPA. Intelligence services, or even individual employees, are given a great deal of discretion in determining whether, and to what extent, a national security exemption should be applied. The lack of certainty about when such an exemption can be applied could result in abuse, inconsistent application and scope creep. This is coupled with the fact that the exemptions work to hamper the oversight role of the ICO, raising concerns for accountability. This is particularly concerning because national security and counter-terrorism laws have long been used, in the UK and abroad, as a pretence to unlawfully expand surveillance authority.[196]

The security breach notification gap

Section 108(1) of the DPA requires intelligence services (when they are the controller) to notify the Commissioner if they become aware of a serious personal data breach.[197] However, they do not have to do so *"if the breach also constitutes a relevant error within the meaning given by section 231(9) of the Investigatory Powers Act 2016"* (IPA).[198]

196 See, e.g., European Center for Not-for-Profit Law, International Network of Civil Liberties Organizations and Privacy International, 'Under Surveillance: (Mis)use of Technologies in Emergency Responses: Global lessons from the Covid-19 pandemic' (Privacy International, 14 December 2022), available at: https://privacyinternational.org/report/5003/under-surveillance-misuse-technologies-emergency-responses-global-lessons-covid-19.

197 DPA 2018 §108(1).

198 IPA 2016 §231(9).

Section 231(9) of the IPA defines a relevant error as an error *"by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment, and which are subject to review by a Judicial Commissioner […]."*[199] The Investigatory Powers Commissioner's Office (IPCO) has included it in its 'useful definitions' resource and defines it as *"an error made by a public authority when carrying out activity overseen by IPCO."*[200]

The effect is that if a data breach also constitutes a 'relevant error' then the intelligence services do not have to report it to the Information Commissioner. However, the IPCO has no powers or functions concerning data protection, and accordingly no relevant enforcement or remedial powers. The effect of this is to circumvent the enforcement and oversight role of the ICO related to data breaches. This gap was noted by IPCO in its 2024 Annual Report:[201]

> *"It is unclear what the rationale is for UKIC [United Kingdom Intelligence Community] avoiding the notification requirement to the ICO, given that we have no functions in relation to data protection compliance and cannot exercise the enforcement powers in Part 6 of the Data Protection Act 2018 (DPA). At present, this means that UKIC could commit a serious personal data breach which might not come to the attention of the competent supervisory authority for data protection unless we refer the matter. Given the possible sensitives involved, we are not best placed to do this. This may leave a gap which could be contrary to the public interest."*

199 Ibid.

200 Investigatory Powers Commissioner's Office, 'Useful Definitions' (IPCO), available at: https://www.ipco.org.uk/investigatory-powers/useful-definitions/.

201 IPCO, 'Annual Report of the Investigatory Powers Commissioner 2024' (n 25).

Human Rights and Equality laws

AI use can result in a breach of the Equality Act 2010 and the Human Rights Act 1998.[202] It can undermine several fundamental rights by enabling intrusive surveillance that threatens the right to privacy, creating opaque or biased decisions that amplify discrimination or hindering the ability to challenge unfair outcomes.[203] Human rights and equality laws apply to the use of AI in the public sector.[204] They guard against these types of harms, and can provide redress in the event of non-compliance. We know they apply to AI, but the nuance of how they should be applied has not yet been thoroughly detailed by UK courts.[205]

This area of law is made up of a patch work of sources: The Equality Act 2010 (the Equality Act), the European Convention on Human Rights[206] (which is incorporated into domestic law through the Human Rights Act 1998), assimilated European Union (EU) law and the common law.[207] Broadly, and together, they provide that everyone should be able to enjoy their rights without discrimination.[208] Human rights laws set out a list of fundamental rights and freedoms that must be respected, protected and fulfilled.[209] Equality laws provide a list of protected characteristics and prohibit certain conduct that discriminates against people with that characteristic. The protected characteristics in the Equality Act include: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race,

202 Equality and Human Rights Commission, 'An Update on our Approach to Regulating Artificial intelligence' (EHRC, 30 April 2024) available at: https://www.equalityhumanrights.com/media-centre/news/update-our-approach-regulating-artificial-intelligence.

203 The impact of AI on human rights, and the ways in which it can undermine or infringe on certain rights has been extensively discussed. See additionally The European Network of National Human Rights Institutions, 'Key Human Rights Challenges of AI' available at: https://ennhri.org/ai-resource/key-human-rights-challenges/. There is also on-going debate about whether we need to reconsider human rights in response to AI. See, e.g., Professor Yuval Shany, 'Expert Comment: Is it time to reconsider our human rights in the age of AI?' (University of Oxford, 2 December 2025), available at: https://www.ox.ac.uk/news/2025-12-02-expert-comment-it-time-reconsider-our-human-rights-age-ai.

204 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 206.

205 Several challenges have been brought concerning the use of AI by public authorities which concerned equality arguments, but they have not resulted in full reasoned judgments. Ibid., 219.

206 European Convention on Human Rights (ECHR), 4 November 1950.

207 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 206.

208 ECHR art. 14.

209 British Institute of Human Rights, 'What duties do public bodies and service providers have?' (British Institute of Human Rights, n.d.), available at: https://www.bihr.org.uk/get-informed/what-duties-do-public-services-have.



religion or belief, sex and sexual orientation.[210] These characteristics could be engaged when data is input into a decision-making system, and when it makes a decision. This was observed by McGurk and Tomlinson who note:[211]

"It is possible to imagine AI and automated systems implicating all of these protected characteristics, either through how they are treated when they constitute inputs into decisions (implicitly or explicitly) or through people with a protected characteristic (or protected characteristics) experiencing adverse outcomes."

They go on to note that within this area, the two legal claims most likely to be brought when AI is used are direct and indirect discrimination.[212] Direct discrimination is when someone is treated less favourably because of a protected characteristic.[213] Indirect discrimination happens when a neutral or objective looking policy or practice applies to everyone equally, but disadvantages certain groups with a protected characteristic.[214]

So, for example, consider if a public body introduces an AI-driven housing-benefit eligibility tool which incorrectly flags anyone over 65 as high-risk for fraud. This could be direct discrimination because anyone over 65 will be treated less favourably due to a protected characteristic (age).

Compare this to an example where a council deploys an AI-driven school admissions programme. The process requires every applicant to submit proof

210 Equality Act 2010 (Equality Act) §4.

211 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 211.

212 B. McGurk and J. Tomlinson, 'Artificial Intelligence and Public Law' (n 153) p. 214.

213 Equality and Human Rights Commission, 'Direct and indirect discrimination' (Equality and Human Rights Commission), available at: https://www.equalityhumanrights.com/equality/equality-act-2010/your-rights-under-equality-act-2010/direct-and-indirect-discrimination, accessed 10 September 2026.

214 Ibid.

of address documents (a neutral policy). However, if the system gives higher priority to those who upload higher resolution documents, this may amount to indirect discrimination. The seemingly neutral policy may put a particular protected group (those linked to socioeconomic disadvantage, which may intersect with race or disability) at a disproportionate disadvantage.

But this distinction can be difficult in the context of AI. As noted by Lord Sales:[215]

> *"A system may be instructed by its programmers to achieve some neutral objective - like accurately predicting recidivism... However, if the operation of the artificial intelligence finds that certain protected characteristics data (like sex, ethnicity or some other protected characteristic) can be used as part of an algorithm that accurately predicts that variable, then it will make decisions in individual cases, at least partly, 'because of' that characteristic. At a system level, this looks like something neutral on its face, that should be capable of justification, yet at an individual level, the system has made a decision because of a protected characteristic. That looks more like direct discrimination: a difference in treatment that is incapable of justification."*

Despite these challenges, equality laws may provide some redress for discrimination that occurs as a result of AI use.

But such redress, as discussed below, will require sufficient transparency and accessibility to decisions to challenge them, which is currently very difficult to achieve in the intelligence context. Human rights specific laws could apply in the event that specific rights are infringed as a result of AI use – for example, the right to an effective remedy[216] may be undermined by the opaque nature of AI decisions which may undermine an individual's ability to challenge outcomes or decisions.[217]

215 Lord Sales, 'Information Law and Automated Governance' (UK Supreme Court, 24 April 2023), available at: https://supremecourt.uk/uploads/Information_Law_and_Automated_Governance_L_Sales_keynote_address_Information_Law_Conference_April_2023_4063da5bfe.pdf.

216 ECHR, art. 13.

217 The impact of AI on human rights, and the ways in which it can undermine or infringe on certain rights has been extensively discussed. See additionally ENNHRI, 'Key Human Rights Challenges of AI' (n 204). There is also on-going debate about whether we need to reconsider human rights in response to AI. See, e.g., Y.Shany, 'Expert Comment: Is it time to reconsider our human rights in the age of AI?' (n 204).

The right to privacy may also be infringed. Such infringement may concern a misuse of someone's personal data – undermining their ability to control information about themselves (discussed above).[218] But it may also extend beyond the data protection concerns often focused on and include infringements due to mass surveillance and the increased intrusiveness of surveillance facilitated by AI. Both raise questions as to whether AI-facilitated surveillance can be necessary or proportionate, and whether the legal regime governing it is sufficient to be in accordance with law. We discuss some of these privacy harms in more detail below when we engage with the sector-specific regulation provided by UK intelligence laws. If the right to privacy is infringed, it often undermines the exercise of concomitant rights such as freedom of expression, freedom of assembly and freedom of association.[219] If someone is aware they are being surveilled, they may censor themselves, choose not to attend a protest or dissociate with certain people or groups.

The application of these laws could apply to all three stages of the AI pipeline, as depicted in the table and infographic attached as appendices 1 and 2.

The application of human rights and equality laws to intelligence agencies

As detailed, these laws can guard against human rights abuses and may provide redress in the event of non-compliance. However, their application in the context of intelligence services may be undermined. This is largely due to additional broad exemptions for national security, and inherent challenges with bringing such a claim.

The national security exemption

The Human Rights Act 1998 (the HRA) applies to intelligence services.[220] Accordingly, it is unlawful for any of them to act in a way that is incompatible

218 Nadav Voloch and Ron S Hirschprung, 'Both Ends of Artificial Intelligence Impact Privacy: a Review of Violation and protection' (Frontiers in Artificial Intelligence, National Library of Medicine, 2026) available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC12957209/.

219 Leith Jeroudi, 'Surveillance and Human Rights' (Geneva Centre for Human Rights Advancement and Global Dialogue, June 2023), available at: https://gchragd.org/wp-content/uploads/2023/06/GCHRAGD-SURVEILLANCE-AND-HUMAN-RIGHTS-background-paper.pdf; see also Privacy International, 'Privacy Matters' (Privacy International), available at: https://privacyinternational.org/learning-resources/privacy-matters accessed 10 September 2026.

220 Intelligence services are not explicitly excluded from the Human Rights Act 1998 (HRA) and would be considered 'public authorities' for the purpose of section 6(3) of the HRA.

with human rights.[221] This would include acts taken involving AI.

However, as we've seen, national security can exempt certain bodies from complying with certain legal obligations, and this is no different with human rights law. The following rights explicitly provide that they may be limited for the purposes of national security:

- the right to a fair trial (only to the extent concerning the public's access to trial);[222]
- the right to respect for private and family life;[223]
- freedom of expression;[224] and
- freedom of assembly and association.[225]

The Equality Act 2010 is also not immune from the national security exemption. Section 192 provides that if someone does something necessary for national security, it won't be a contravention of the Act. It provides:

> *"A person does not contravene this Act only by doing, for the purpose of safeguarding national security, anything it is proportionate to do for that purpose."*

Built into this section is therefore the requirement that the discrimination must be proportionate.[226] This broadly requires that any restriction on a person's rights must pursue a legitimate aim, use the least restrictive means, and strike a fair balance between individual rights and the interests of others.[227]

221 HRA §6(1).

222 ECHR art. 6, incorporated into HRA §1(1).

223 ECHR art. 8, incorporated into HRA §1(1).

224 ECHR art. 10, incorporated into HRA §1(1).

225 ECHR art. 11, incorporated into HRA §1(1).

226 Equality and Human Rights Commission, 'Exceptions where equality law applies differently' (29 June 2021) available at: https://www.equalityhumanrights.com/equality/equality-act-2010/dismissal-redundancy-and-retirement/exceptions-where-equality-law.

227 British Institute of Human Rights, 'The Principle of Proportionality' (British Institute of Human Rights), available at: https://www.bihr.org.uk/get-informed/legislation-explainers/what-is-proportionality.

Challenges with bringing a claim under equality law

Even if no such exemption applies, and you can rely on equality law, establishing the grounds for a challenge are hard. Even outside of the context of intelligence agencies, understanding whether bias exists, and obtaining the relevant information may be a challenge. This was succinctly stated by barrister Melissa Stock in her recent commentary on the court's decision in *R (Bridges) v The Chief Constable of South Wales Police*[228] (a case concerning bias in the police's use of facial recognition technology). She was remarking in the context of law enforcement use and noted:[229]

> *"[N]ot only are false positive matches a problem. If bias already exists within the software, there is also no way of knowing how many false negative results exist, with or without human intervention at the output stage. However, it will be difficult to independently assess the issue of bias, because it requires the police force (or relevant public authority) to have access to the datasets that were used to train the AFR [automated facial recognition] system. The developers of AFR software will consider such data, and the algorithms it applies, to be commercially sensitive information and they may be reluctant to reveal it."*

Consequently, although equality law puts guardrails in place to protect human rights and guard against discrimination, its application to intelligence services may be circumvented by the national security exemption.

Bringing a claim under the Human Rights Act

Bringing a claim under the HRA could be more feasible, primarily because proving an interference with, for example, the Article 8 right to privacy or the Article 10 right to free expression is easier than proving bias to a legal standard (even when and if bias is anecdotally observed).

The European Court of Human Rights' caselaw establishes that many of the forms of data collection and surveillance already discussed, for example, the

228 *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA CIV 1058.

229 Melissa Stock, Privacy law Barrister, '*R (Bridges) v the Chief Constable of South Wales Police* [2020] EWCA CIV 1058', available at: https://privacylawbarrister.com/2020/08/28/r-bridges-v-the-chief-constable-of-south-wales-police-2020-ewca-civ-1058/.

collection of sensitive information like personal communications, constitutes an interference with the right to privacy.[230] Although national security is a legitimate interest that the government can use to restrict the rights provided in the HRA, this restriction must be necessary, proportionate and governed by law.[231]

Indeed, the UK Investigatory Powers Act (IPA) has been subject to an HRA challenge. Liberty, a UK campaigning organisation, sought to judicially review the UK government's ability to exercise 'bulk powers' under the IPA and collect massive amounts of data from telecommunications providers. The challenge alleges violations of the rights to privacy and freedom of expression as enshrined in the ECHR, and seeks a declaration of incompatibility under the HRA.[232] Initially, the UK High Court held that the bulk powers do not violate privacy and free expression because they are proportionate, which was confirmed by the Court of Appeal, with one exception, in 2023.[233] Liberty have appealed to the European Court of Human Rights.[234] Although this case was not initially successful in its HRA claims, Liberty were not precluded from bringing the claim due to national security exemptions or their inability to obtain evidence. However, it is worth noting that without the 2013 Edward Snowden leaks, the IPA might not exist, making it much more difficult to challenge the bulk powers it includes.[235]

Privacy International has also attempted to challenge MI5's data-handling arrangements before the Investigatory Powers Tribunal.[236] In mid-2019, MI5

230 See, e.g., *Szabó and Vissy v Hungary*, App no 37138/14 (ECtHR, 12 January 2016); *Roman Zakharov v Russia* (GC), App no 47143/06 (ECtHR, 4 December 2015).

231 Privacy International, 'Legality, Necessity and Proportionality' (Privacy International), available at: https://privacyinternational.org/our-demands/legality-necessity-and-proportionality, accessed 10 September 2026.

232 Liberty, 'Legal challenge: Investigatory Powers Act' (Liberty), available at: https://www.libertyhumanrights.org.uk/issue/legal-challenge-investigatory-powers-act/, accessed 10 September 2026.

233 *R (National Council for Civil Liberties) v Secretary of State for the Home Department* [2023] EWCA Civ 926.

234 The National Council for Civil Liberties against the United Kingdom, app. no. 15250/40, communicated on 12 March 2026, available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-249612%22]}.

235 See Intelligence and Security Committee of Parliament, 'Privacy and Security: A modern and transparent legal framework' (Intelligence and Security Committee of Parliament, 12 March 2015), available at: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf; David Anderson QC, 'A Question of Trust: Report of the Investigatory Powers Review' (GOV.UK, 11 June 2015), available at: https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review; David Anderson KC, 'Independent Review of the Investigatory Powers Act 2016' (GOV.UK, June 2023), available at: https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016--2/independent-review-of-the-investigatory-powers-act-2016-accessible#fn:6.

236 Privacy International, 'MI5 ungoverned spaces challenge' (n 4).

admitted that personal data was being held in *"ungoverned spaces"*.[237] Much about these 'ungoverned spaces', and how they would effectively be *"governed"* in the future, remained unclear.[238] We argued that these lax data handling arrangements resulted in the systematic violation of the rights to privacy and freedom of expression.[239] The IPT found[240] that MI5 unlawfully retained huge amounts of personal data between 2014 and 2019.[241] During that period, and as a result of these breaches, warrants issued by subsequent Home Secretaries were unlawful.[242]

This win at the IPT, which was facilitated in part by the IPCO's surfacing of some of these concerns in their 2019 report,[243] illustrates why both adequate regulation and robust oversight mechanisms are essential to address concerns about artificial intelligence.

237 Ibid.

238 Ibid.

239 Ibid.

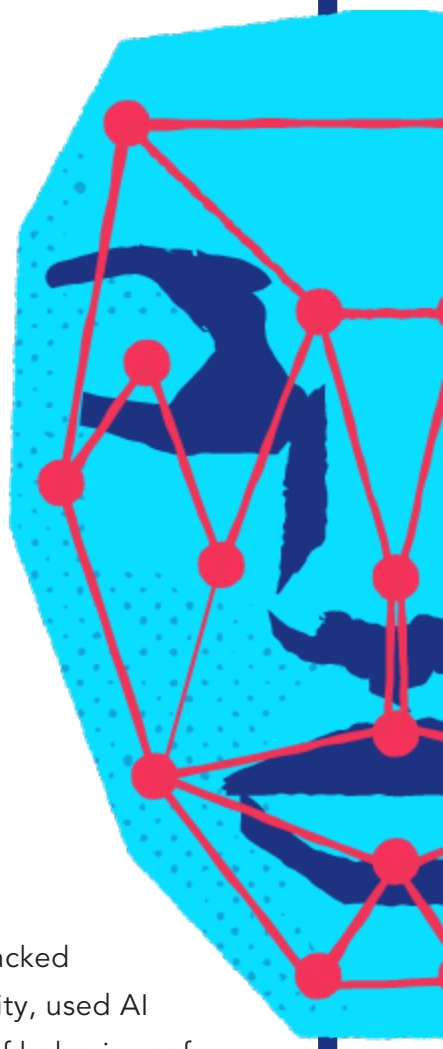
240 Privacy International, 'Press: Landmark ruling exposes years of rule breaking MI5', (Privacy International, January 2023), available at: https://privacyinternational.org/press-release/5027/press-landmark-ruling-exposes-years-rule-breaking-mi5

241 Ibid.

242 Ibid.

243 Investigatory Powers Commissioner's Office, 'Annual Report of the Investigatory Powers Commissioner 2019' (Investigatory Powers Commissioner's Office, December 2020) available at: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf, pp. 37-38.

FACIAL RECOGNITION TECHNOLOGY AS A CASE STUDY



Facial recognition technology (FRT) is a form of AI-enabled surveillance that we consider constitutes a severe violation of the right to privacy, and which is not sufficiently regulated (or indeed, even explicitly mentioned) by the IPA or RIPA. As a result, safeguards such as the need to obtain prior authorisation before using FRT, restricting the use of certain forms of FRT, and restricting the use of FRT at certain times, such as outside of polling stations, are markedly absent.

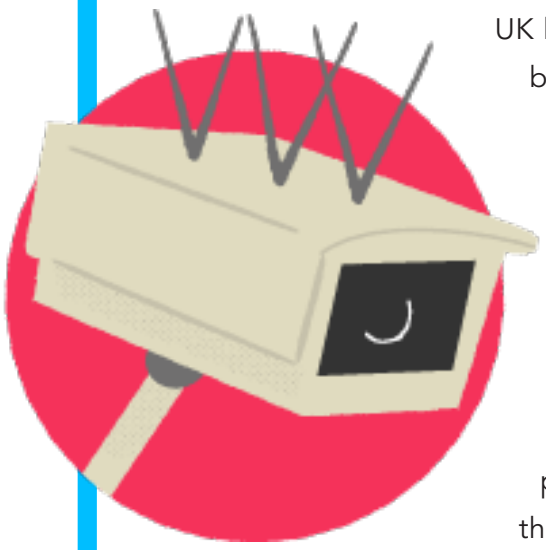
Although not always conceived of as such, FRT is AI – a camera scans your face, and AI uses identifying markers to compare it to faces in one of myriad databases.[244] Police in the UK are quickly adopting technology (FRT) in their law enforcement practice, [245] but intelligence agencies in the UK almost certainly also use the technology in conjunction with other forms of AI-enabled data analysis. For example, the Financial Times reported that sources familiar with the matter claim that Israel and the United States hacked into traffic cameras in Tehran by exploiting a technical vulnerability, used AI to comb through millions of hours of footage, identify patterns of behaviour of senior officials, and mapped their movement through Tehran.[246] The US and Israel

244 Privacy International, 'Facial Recognition' (Privacy International), available at: https://privacyinternational.org/learn/facial-recognition.

245 See, e.g., Information Commissioner's Office, 'Facial recognition in policing: earning public trust through strong data protection governance' (Information Commissioner's Office, 18 August 2026), available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/08/facial-recognition-in-policing/; Home Office, 'Police use of facial recognition: factsheet' (GOV.UK, 4 December 2025), available at: https://www.gov.uk/government/publications/police-use-of-facial-recognition/police-use-of-facial-recognition-factsheet.

246 Mehul Srivastava and Christopher Miller, 'New AI espionage powers trigger Putin camera scare' (Financial Times, 8 June 2026), available at: https://www.ft.com/content/6f4d806c-eb22-4c32-8352-b82692d30e9f.

purportedly used this information in the assassination of Ayotallah Khamenei.[247] While the AI applied to this footage may not have been FRT, FRT could just as easily be used on camera footage. Intelligence agencies in the UK likely possess the same capabilities, and are assisted by the massive number of CCTV cameras in the UK, some of which are enabled with live FRT.[248]



We are concerned that these technologies pose a major risk to human rights, especially the right to privacy and associated rights. If people are aware they are being surveilled, they may alter their behaviour, dissociate with certain groups or avoid attending a protest (where, police do extensively use FRT) – undermining their rights to freedom of expression, assembly and association.[249] Use of this technology may also be discriminatory, as demonstrated by a recent report which revealed bias in police facial recognition technology because it's *"more likely to flag black and Asian people than their white counterparts."*[250]

The unchecked proliferation of FRT, and the ability of intelligence agencies to use FRT in conjunction with the massive amounts of data they already have is just one example of how AI is being used to quickly degrade our right to privacy, and just one reason why laws need urgent reform.

247 Ibid.

248 Privacy International, 'Privacy International's Submission to the UK Home Office Consultation on a Legal framework for law enforcement use of biometrics, facial recognition and similar technologies' (Privacy International, February 2026), available at: https://privacyinternational.org/sites/default/files/2026-03/PI%27s%20response%20to%20the%20UK%20Home%20Office%20consultation%20on%20facial%20recognition%20technology.pdf, p. 1.

249 Ibid., p. 11.

250 Ibid., p. 2.

Intelligence laws

It is important to note at the outset that the regulatory framework that governs intelligences services is complex.[251] We focused primarily on the Investigatory Powers Act 2016 (IPA) but there are several (often overlapping) laws and codes which make it difficult to navigate. Even the IPCO – the body that oversees the use of investigatory powers - has remarked on the complexity of the legal framework, noting:[252]

> *"At present, there is a complex patchwork of legislation that can be difficult to apply to real operational scenarios and difficult to oversee."*

This prompted IPCO to recommend longer term reform of the IPA, suggesting that the Home Office consider *"the broader codified approach to the legislation to enable clarity."*[253] This recommendation was made after the latest round of amendments to the IPA.[254]

These 2024 amendments are the latest step in a long history of changes to the regulation of intelligence. Legal scholar Bernard Keenan categorises the history of the regulation of communications surveillance in the UK as having three distinct phases:[255]

- First, from the foundation of the Post Office (around 1660) until 1985 it was characterised by administrative secrecy;

251 For example, the Regulation of Investigatory Powers Act 2000 (RIPA), which although was largely replaced by the IPA, still governs certain elements including covert human intelligence and some aspects of encrypted electronic data. For more on the relationship between RIPA and the IPA, see: LexisNexis. 'RIPA 2000 (UK) after the Investigatory Powers Act 2016: CHIS, covert surveillance and encryption key disclosure powers', 2026, available at: https://www.lexisnexis.com/en-gb/legal/guidance/regulation-of-investigatory-powers-under-ripa-2000

252 IPCO, 'Annual Report of the Investigatory Powers Commissioner 2024' (n 25) p. 19.

253 Ibid.

254 The Investigatory Powers Act 2016 was amended by the Investigatory Powers (Amendment) Act 2024. It received Royal Assent on 25 April 2025, and most provisions came into force on 14 October 2024. See additionally UK Parliament, 'The Investigatory Powers (Amendment) Regulations 2024' (legislation.gov.uk, 2024), available at: https://www.legislation.gov.uk/uksi/2024/1021/made.

255 Bernard Keenan, 'From Interception to Integration: Encryption, Bulk Data, and the Investigatory Powers Regime' Kings Law Journal, 2025 Vol. 36 No.3, 508 – 539, available at: https://www.tandfonline.com/doi/pdf/10.1080/09615768.2025.2551419.

- Second, from 1985 – 2016 it was marked by legislative obfuscation; and
- Third, since 2016 it has had a conditional form of transparency evidenced by the passing of the Investigatory Powers Act in 2016 (IPA) following the Snowden revelations.

Keenan asserts that the recent changes to the regulatory framework signal

> *"the increasing power of 'surveillance intermediaries' – privately owned communication platforms, primarily located in the United States – and the rise of commercial providers of intelligence analytics."*[256]

His hypothesis is that *"the era of state interception of communications is giving way to an era of state integration with private intermediaries."*[257] Intermediaries are third parties that collect information, typically for their own business purposes, that the government wants.[258] The government seeks that information from the third party, instead of the target directly. It is now *"easier and cheaper to access structured sources of data generated commercially."*[259] This growing dependence on intelligence intermediaries is evidenced through the introduction of third-party bulk dataset warrants and datasets that have a low or no expectation of privacy, discussed below.

We proffer that these changes signal that we are entering a fourth phase of regulation that prioritises the interdependent relationship between big data and AI. Big data supplies the volumes of information needed for models to spot patterns, make predictions and improve. AI tools collect, clean, organise and analyse that data – identifying patterns, anomalies and trends.

Intelligence laws have been amended to account for this interdependent relationship – enhancing the Government's surveillance powers and enabling greater access to data. This is evidenced by a regulatory framework that seems to prioritise mass data collection evident through:

256 Ibid., p. 508.

257 Ibid.

258 Ibid., p. 516.

259 Ibid., p. 529.

1. Weakened safeguards that apply to a new category of bulk personal data – datasets that have a low or no expectation of privacy;[260]
2. Permitting access before authorisation for datasets held by third parties; and
3. Empowering intelligence agencies to require companies to build back doors.

Despite enabling increased collection, the amendments to the IPA did not include any safeguards to mitigate against the novel risks posed by intelligence services' use of AI. As a result, the newly amended IPA comprises a regulatory framework that enables and encourages the use of AI but doesn't mitigate the risks.

How the Investigatory Powers Act governs AI

The IPA does not mention AI explicitly and is drafted to be technologically neutral. Our research shows that it predominantly governs stage 1 – data collection. Data protection law, and human rights and equality laws pick up most of the regulatory slack for the other stages – and we have discussed how limited that is. This section provides a high-level overview of how the IPA governs each stage of the AI pipeline. A more detailed discussion of some of the regulatory concerns and gaps is provided in section 2.3 below.

Stage 1: data collection

The collection of data by UK intelligence agencies is predominantly regulated by requirements to obtain warrants authorising that collection. Such warrants typically require a two-stage approval process (known as the *"double-lock"*) which requires authorisation from the Secretary of State and approval from a Judicial Commissioner. While warrants can be an effective restraint, the law enables instances that permit the bypassing of such warrants (see the urgency carve-out and third-party datasets discussed in section 2.3 below) or authorises the issuance of bulk warrants which insufficiently restrain subsequent use of the data collected. Notably, the law doesn't provide any constraints or safeguards regarding using AI to actually obtain the data and fails to include requirements that enable AI's use to be interrogated at the authorisation stage.

260 IPA pt 7a.

Stage 2: making the data useable

The law does not explicitly include AI-specific safeguards for stage 2. There are no requirements related to preprocessing, data integration, synthetic data generation or labelling. Arguably such issues may be considered in the required necessity and proportionality assessments. They may also be considered in terms of data protection principles that personal data must be adequate, relevant,[261] accurate and up to date.[262] However, we have seen how easily these data protection requirements may be circumvented.

It appears permissible that data collected under one warrant can be integrated with data collected under other warrants or powers. These could be merged into one analysis platform without additional authorisation. Merging datasets and applying AI analysis raises several concerns that the IPA does not address. Combining datasets can amplify biases already present in underlying data, leading to discriminatory or skewed outcomes,[263] while also increasing the likelihood of false correlations where individuals are linked to suspicious activity based on weak or coincidental patterns. The merging of datasets also could create intrusive and detailed profiles of individuals,[264] and increases the chance of re-identification of anonymised data,[265] heightening privacy concerns.

It is not immediately clear whether the safeguards relating to examination of material[266] meaningfully mitigate these concerns. They appear to limit examination to whether it is necessary and proportionate,[267] but no additional safeguards consider the assessment of new risks posed by merging large datasets.

261 DPA §85(1)(C).

262 DPA §85(1)(D).

263 Joanna Redden, Jessica Brand and Vanesa Terzieva, 'Data Harm Record' (Data Justice Lab, August 2020), available at: https://datajusticelab.org/project/data-harm-record/.

264 Ibid.

265 National Cyber Security Centre 'Security Principles for Protecting the Most Sensitive Personal Information in Datasets', available at: https://www.ncsc.gov.uk/collection/security-principles-protecting-most-sensitive-personal-information-in-datasets/principle-6-when-merging-data-check-if-spi-becomes-exposed.

266 IPA §152.

267 IPA §152(1).

Stage 3: using the data

The IPA provides limited safeguards with respect to the analysis of data once it is collected, and none specifically address AI use. Two notable forms of regulation in this stage are the requirement to seek examination warrants for certain searches of bulk data[268] and to approve of the selectors used in that examination, as required by the European Court of Human Rights Grand Chamber judgment in *S and others v the UK*.[269] Below, we address in more detail how both must be adapted to the new challenges presented by AI.

Also falling within this stage, collected data may be used for *"testing or training activities."*[270] The expanded definition does not explicitly say AI training, but it could be read to permit AI development.[271] Yet there are no safeguards aimed at controlling such development.

The UK also does not have any form of regulation that assesses the risk profile and/or prohibits particular use cases of AI (e.g. using AI for a social scoring system). Such a risk-based approach is used in the European Union's Artificial Intelligence Act (EU AI Act).[272] Notably, some of the AI systems prohibited in the EU AI Act include:[273] 1) systems that assess the risk of an individual committing criminal offences solely based on profiling; 2) social scoring (i.e. to evaluate or classify people or groups based on behaviour); and 3) real-time biometric identification in public spaces. These are exactly the kinds of uses we expect of the intelligence services, however, the EU AI Act also includes a broad exclusion for national security, and intelligence agencies in the EU reportedly use AI in similar ways to the UK.[274] As we address in our recommendations at the end of this paper, we think certain AI use cases are so intrusive on privacy and other rights that they should never be permitted.

268 IPA pt 2, ch 1 (15(3)); pt 5 ch 1 (99(9)); pt 6 ch 1 (152); pt 6 ch 3 (193).

269 *Big Brother Watch and others v The United Kingdom* (25 May 2021) application nos. 58170/13, 62322/14 and 24960/15, paras 354-356.

270 IPA §17(2)(c).

271 IPA §17(3).

272 EU AI Act Regulation (EU) 2024/1689 available at: https://artificialintelligenceact.eu/ai-act-explorer/.

273 EU AI Act, ch II art 5.

274 EU AI Act, art 2(3) which excludes from its scope "AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities."

2.3 UNPACKING SPECIFIC REGULATORY CHALLENGES AND GAPS

This section explores some of the key regulatory gaps and governance concerns that AI poses for the existing legal regime – specifically the IPA.

No interrogation of AI involvement or duty to disclose

The collection of data is typically regulated by the IPA through different authorisation mechanisms – for example, to collect bulk data held by a third party, a warrant must be issued by the Secretary of State and approved by a Judicial Commissioner.[275] However, what the IPA seems to miss in this authorisation stage is a duty to disclose and interrogate the use of AI in the decision to apply for a warrant.

In most instances, an agency submits a request to the Secretary of State who considers whether a warrant may be issued.[276] The law specifies that they consider: whether it is necessary;[277] that the conduct is proportionate;[278] that the safeguards relating to retention and disclosure are in force;[279] and whether it is urgent.[280] The Act does not contemplate a scenario where the application for a warrant, the assessment of necessity, or the proportionality analysis is itself AI-assisted or AI-generated. If intelligence services use AI systems to identify people of interest, draft warrant applications, or recommend that warrants be sought, the law places no requirements on the quality, transparency, or audibility of the AI system that informed those decisions. There are no requirements that they disclose these details or report any concerns around error rates, low-quality data, or unrepresentative data. There are also no requirements that the human decision-maker interrogate or show evidence

275 Part 7B of the Investigatory Powers Act 2016. See also: Part 6, and Part 2 which also require the double-lock authorisation.

276 See IPA §19.

277 IPA §19(1)(a).

278 IPA §19(1)(b).

279 IPA §19(1)(c).

280 IPA §19(1)(d).

that they have interrogated an automated decision. The lack of disclosure requirements makes it impossible to interrogate AI's involvement.

This is not cured by the second leg of the double-lock – Judicial Commissioner approval. There was debate during the passage of the IPA resulting in a more robust review than the plain text that the IPA suggests - that the Judicial Commissioner only apply the same principles as would be applied by a court on application for judicial review.[281] Instead, Judicial Commissioners must review the necessity and proportionality of the warrant so as to ensure it complies with the duty to protect individuals' privacy.[282] Although this review is relatively robust, it does not account for the possibility that requesting agents are relying on AI generated or analysed information. When the underlying intelligence that supports a warrant application has been generated by an AI system, through pattern-matching across bulk datasets, behavioural profiling, or predictive analytics, the Judicial Commissioner has no clear statutory basis for interrogating the AI systems methodology, training data, error rate, or potential for bias. The review standard is inadequate because it defers to the requester's factual premises, and AI-generated premises may be opaque or not disclosed.

This raises the question – at what stage will AI's involvement in important decisions be interrogated?

A decision that someone is a subject of interest and should therefore be subjected to continuous, intrusive surveillance is an important one. And one which has significant implications for their right to privacy. Of course, these are not new decisions, but AI's involvement in them is – and it raises new and profound risks.

IPCO is 'interested' in understanding these risks
Their Scope of Interest in AI noted:[283]

> *"IPCO is principally interested in understanding how the use of AI may increase the number of subjects of interest who can be investigated by public authorities and how the use of AI may change*

281 IPA §23(2)(a).

282 Investigatory Powers Commissioner's Office, 'Authorisations', available at: https://www.ipco.org.uk/what-we-do/the-double-lock/, accessed 10 September 2026.

283 IPCO, 'IPCO's Scope of Interest in AI' (n 5).

any intended or collateral intrusion on a persons' rights to privacy.

This interest starts with how AI may have been used to help prepare an application to use one of the powers, how it has been used in relation to any conduct authorised under the investigatory powers regime ('collection'), how the information obtained by the conduct is then used ('analysis') and managed (safeguarding')."

We hope this interest addresses these profound risks.

The urgency carve-out

In most instances, the collection of data by intelligence agencies requires a warrant. To obtain a warrant, authorisation by the Secretary of State and judicial approval are generally required - this is known as the *"double-lock"*. However, in every warrant regime in the IPA[284] prior approval by the Judicial Commissioner can be dispensed with if there is *"an urgent need."*[285] Whether there is urgency is subjectively determined by the issuing authority. The warrant takes effect and the Judicial Commissioner has three working days to decide whether to approve or refuse the decision to issue the warrant.[286]

However, material obtained during that three day window remains lawful, even if approval is refused.[287] The IPA does not mandate the deletion of this material – the Judicial Commissioner has a discretion to direct destruction and they may impose conditions on its use or retention.[288] Accordingly, data could be collected under the pretence of urgency and could still be relied on even if the Judicial Commissioner later refuses to approve the

284 This includes: Section 24 - targeted interception, targeted examination & mutual assistance; Section 109 - targeted equipment interference, Section 180 - bulk equipment interference, Section 209 - specific bulk personal data warrants; section 226BB - individual Part 7A authorisations, and section 226GB - third-party bulk personal data warrants.

285 See, e.g., section 24(1) of the IPA which concerns chapter 1 warrants (targeted interception warrants, targeted examination warrants and mutual assistance warrants).

286 IPA §24(3).

287 IPA §25(8)(a).

288 IPA §25(3).

warrant. Nothing in the IPA appears to prevent serial reliance on urgency.

This urgency carve-out is particularly problematic in the context of AI if such data has already been processed, or used to train a model. Keenan remarked on this in the context of datasets with a low or no expectation of privacy, noting:[289]

> *"[e]ven if approval is subsequently refused the algorithmic analysis will already have occurred. Such information cannot be 'unprocessed' by an AI model that has examined it. It is not clear that the refusal of permission would also necessitate the deletion of any model unlawfully built on mis-classified datasets."*

The IPCO reports on the number of authorisations granted,[290] which includes how many of those were urgent, but it does not appear to disclose how many were issued under urgency and refused by a Judicial Commissioner.

Datasets with a low or no expectation of privacy



The amended IPA now includes a provision on the collection and retention of a new category of data - bulk personal data sets about people that have 'a low or no expectation of privacy.'[291] Unlike the collection of other datasets, these don't require a warrant to authorise collection, just approval from a Judicial Commissioner (serving or retired Judge). But what

289 Bernard Keenan, 'From Interception to Integration: Encryption, Bulk Data, and the Investigatory Powers Regime' Kings Law Journal, (n 254) p. 533.

290 See for example, page 68 of the Investigatory Powers Commissioner's Annual Report 2024 which provides that 5,814 directed surveillance authorisations were made in 2024 were made by law enforcement agencies, public authorities, local authorities and prisons, 499 of which were made under urgent provisions, available at: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2024.pdf.

291 IPA §226A(1). For more on the EU AI Act and how it regulates facial recognition technology, see Privacy International, 'Toward Regulation: Addressing the Legal Void in Facial Recognition Technology' (1 October 2025) available at: https://privacyinternational.org/long-read/5682/toward-regulation-addressing-legal-void-facial-recognition-technology.

are these datasets? Could they include everything you've ever published online and on social media? Probably. Maybe. It's not certain because the law does not specify a list of datasets that qualify as having 'low or no expectation of privacy.' Instead, it lists several factors[292] that should be considered in determining whether a data set qualifies. A lot of these factors focus on the public nature of the data, seemingly treating publicly available data as carrying low privacy expectations.

The courts have long recognised that there is a *"zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."*[293]

Understanding the bounds of private and public in the context of Article 8 (the right to privacy) of the European Convention on Human Rights (ECHR) is complex. The ECtHR has acknowledged that some 'public' engagements may be considered private for the purposes of Article 8. In *Peck v the United Kingdom*, the ECtHR noted:[294]

> *"Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. That Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."*

The ECtHR has also acknowledged that the expectations of privacy may change when a 'systematic or permanent record' exists. Specifically, it has noted:

> *"There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a*

292 IPA §226A(3) provides these lists of factors which include: the nature of the data, the extent to which it has been made public, individual consent to it being made public, its subjection to editorial control, the extent to which it is known about and whether it has already been used in the public domain.

293 *Peck v the United Kingdom*, App no 44647/98 (ECtHR, 28 January 2003).

294 Ibid., para 57; see also, *P.G. and J.H. v United Kingdom*, App no 44787/98 (ECtHR, 25 September 2001).

> *person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain."*

Because of this, the ECtHR has held that the compilation of data by security services on particular individuals, even without using covert surveillance, was an interference with their private lives.[295]

Defining what data falls within this category is complex, and without a defined scope may be open to abuse, or scope creep. The IPCO raised concerns with the approach taken to defining these categories[296] and asserted that the use of data for capability development and machine learning models is not indicative of a low/no reasonable expectation of privacy.[297]

These questions become even more complex when AI analysis is involved. Raw data that is *"public"* may become more private after AI analysis. For example, public social media posts, when processed through sentiment analysis and natural language processing could reveal someone's political beliefs and psychological profiles. Further, multiple harmless, or even anonymous, pieces of data can be aggregated or analysed with other datasets to reveal more sensitive information. This is known as the mosaic effect[298] which *"suggests that even anonymized data, which may seem innocuous*

295 *Rotaru v Romania*, (GC) App no 28341/95 (ECtHR, 4 May 2000) §§ 43-44; *Amann v Switzerland* [GC], App no 27798/95 (ECtHR, 16 February 2000) §§ 65-6.

296 IPCO, 'Annual Report of the Investigatory Powers Commissioner 2024' (n 25) p. 19.

297 Ibid.

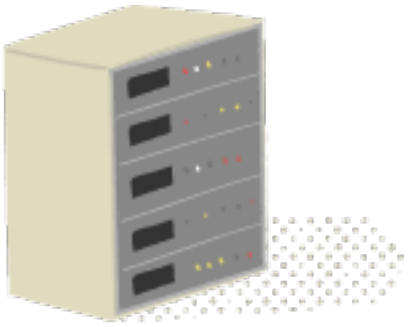
298 Centre for humdata, United Nations Office for the Coordination of Humanitarian Affairs, 'Mosaic Effect', available at: https://centre.humdata.org/glossary-2/mosaic-effect/, accessed 10 September 2026.

in isolation, may become vulnerable to re-identification if enough datasets containing similar or complementary information are released."[299]

These datasets with low or no expectations of privacy are apparently essential for training AI tools,[300] and their introduction reflects the reliance of intelligence agencies on third party intermediaries. As noted by Keenan:[301]

> *"[i]t is an error to imagine BPDs [bulk personal datasets] as if they are static datasets only containing historic data. They include rolling streams of new data. This point is encoded in the legislation: an authorization for the use of a 'low/no' BPD also applies to any 'replacement' datasets 'that do not exist at the time of the grant of the authorization but may reasonably be regarded as replacements for' the original dataset. A BPD is in this way not so much a discrete object as an interface that integrates the systems of the intelligence services with the data feeds provided by surveillance intermediaries that gather and agglomerate different types of bulk data."*

The 2024 Amendments thus reduced safeguards on datasets with 'low or no expectation' of privacy at a time when AI likely makes that data even more revealing and useful. This is another significant gap in the regulatory regime which is exacerbated by AI.



Third party bulk personal datasets

Part 7B of the IPA concerns third party bulk personal datasets.[302] These are datasets that are held by a third party and examined by intelligence services in situ (i.e. on the third-

299 Ibid.

300 Bernard Keenan, 'From Interception to Integration: Encryption, Bulk Data, and the Investigatory Powers Regime' Kings Law Journal, (n 254) page 533.

301 Ibid.

302 IPA §266E.

party's system).[303] The data is not obtained or retained by the intelligence services.[304] Part 7B allows intelligence services to access this data before obtaining a warrant.[305] They may do so in order to carry out an initial inspection to assess whether the dataset includes personal data,[306] or to assess its value, or operational requirements.[307] Notably, during this warrant-free initial inspection, intelligence services are permitted to analyse some of the data on their own systems. The Code of Practice on these datasets[308] explicitly provides:[309]

> *"As part of the initial assessment of value, it may be necessary to run data outputs from the 3PD [third party bulk personal dataset] under inspection through separate systems controlled by the intelligence service, for the sole purpose of assessing the potential value of the dataset. This may allow a fuller assessment of the necessity and proportionality of access to data to be made and inform the decision as to whether to seek a 3PD warrant."*

This *"access without acquisition model"* creates three regulatory risks. The first, and most obvious, is that it enables access before authorisation and therefore creates a regulatory backdoor. Although the law restricts the purpose of these inspections to the assessment of value[310] there is no clear technical limitation of what this means, and there are no safeguards in place to ensure this purpose limitation. Data is still being handled, processed and analysed (which is even permitted on 'separate systems controlled by the intelligence services'), and insights could be generated or data retained. Second, allowing intelligence services to run this data in their own systems creates two risks – 1) that the data will be combined with existing internal datasets to make inferences or generate intelligence, and 2) if

303 Home Office, 'Intelligence services' use of third party bulk personal datasets: code of practice' (GOV.UK, 6 June 2025), available at: https://www.gov.uk/government/publications/third-party-bulk-personal-datasets-code-of-practice/intelligence-services-use-of-third-party-bulk-personal-datasets-code-of-practice-accessible.

304 Ibid., para 2.3.

305 Ibid., para 2.14.

306 IPA §226I(2).

307 Home Office, 'Guidance: Intelligence Services' (n 302), para 2.15.

308 Ibid.

309 Ibid., para 2.17.

310 IPA §226I.

AI is used, it may be impossible to make it forget, or 'unprocess' the data.[311] Of course, whether the AI *"remembers"* what it *"learned"* when analysing the third party dataset depends on the system and its limitations, but there are insufficient safeguards provided in the law to guard against these risks. The third risk is closely related - the law does not seem to acknowledge or even name this liminal data acquired during the initial inspection of the third party data. Consequently, such data may entirely circumvent any requirements relating to retention or deletion.

Technical Capability Notices

Technical Capability Notices (TCN), provided for by section 253, empower the Secretary of State to issue secret notices to operators which impose obligations on them,[312] and require them to take specified steps to meet those obligations.[313] Their purpose is to *"ensure that the operator is capable of providing assistance in giving effect to an interception warrant, equipment interference warrant, or a warrant or authorisation for obtaining communications data issued under the [IPA]."*[314] Essentially, they require operators to engineer or adapt systems to make surveillance possible. They can require the building of a backdoor. For this reason, they have been described as *"among the most intrusive and secretive measures in the U.K.'s surveillance regime."*[315]

TCN's are issued by the Secretary of State and require approval from a Judicial Commissioner[316] (the *"double-lock"*). They may be issued to 'Operators' who include postal operators, telecommunications operators or those proposing to become either.[317] The definition of telecommunications operators in the IPA is

311 Rachel Layne, 'How to Make AI 'Forget' All the Private Data It Shouldn't Have' (Harvard Business School Working Knowledge, 22 February 2024), available at: https://www.library.hbs.edu/working-knowledge/qa-seth-neel-on-machine-unlearning-and-the-right-to-be-forgotten.

312 IPA §253(2)(a).

313 IPA §253(2)(b).

314 Explanatory Memorandum to the Investigatory Powers (Technical Capability) Regulations 2018 No. 353, available at: https://www.legislation.gov.uk/uksi/2018/353/pdfs/uksiem_20180353_en.pdf.

315 Iannis Kouvakas, 'You Can't Have Your Apple and Eat It Too: Decryption Orders and the Perilous Future of U.K. Data Adequacy', U.K. Const. L. Blog (13 March 2025) available at https://ukconstitutionallaw.org/.

316 IPA §254.

317 IPA §253(3).

broad[318] and could include network operators (e.g. Vodafone or BT/Openreach), internet service providers (e.g. Sky Broadband), online communication service providers[319] (e.g. WhatsApp, Gmail or Zoom), or cloud infrastructure providers involved in communication[320] (e.g. Amazon Web Services or Google Cloud). Notably, Operators are not limited to those in the United Kingdom. TCNs can be given to persons (which includes juristic people and likely public bodies) anywhere in the world[321] (so long as they have sufficient connection to the UK).[322]

The obligations that may be specified in a TCN are detailed in the IPA[323] and regulations,[324] and may include:

> *"(a) obligations to provide facilities or services of a specified description;*
>
> *(b) obligations relating to apparatus owned or operated by a relevant operator;*
>
> *(c) obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data;*
>
> *(d) obligations relating to the security of any postal or telecommunications services provided by a relevant operator;*
>
> *(e) obligations relating to the handling or disclosure of any information."*

One of these obligations explicitly allows TCNs to require the removal of electronic

318 IPA §261.

319 IPA §261(13).

320 IPA §§261(10)(b) and (c).

321 IPA §261(8).

322 Privacy International, 'Our Challenge Against UK's Secret TCN Powers', (13 March 2025) available at: https://privacyinternational.org/long-read/5547/our-challenge-against-uks-secret-tcn-powers.

323 IPA §253(5).

324 The Investigatory Powers (Technical Capability) Regulations 2018, No. 353 available at: https://www.legislation.gov.uk/uksi/2018/353/schedule/1/made.



protection which could include encryption. This is assumedly what happened when a TCN was reportedly[325] served on Apple in 2025, requiring them to facilitate global access to end-to-end encrypted user data stored on iCloud.[326] We say assumedly because TCNs are subject to strict secrecy. The IPA requires that the recipient *"must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State."*[327]

The secret nature of TCNs makes it impossible for users of certain services to know how their communications could be affected. They also don't appear to apply on a case-by-case basis, instead, such system-wide changes could enable indiscriminate access, raising necessity and proportionality concerns. The issue of indiscriminate access was considered by The European Court of Human Rights in the matter of *Podchasov v Russia*.[328] In that case, the Russian Federal Security Service (FSB) required Telegram to decrypt and grant access to the communications of six users. The Court noted:[329]

> *"in order to enable decryption of communications protected by end-to-end encryption, such as communications through Telegram's "secret chats", it would be necessary to weaken encryption for all users. These measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications."*

325 Joseph Menn, 'U.K Orders Apple to Let it Spy on Users' Encrypted Accounts' (The Washington Post, 7 February 2025) available at: https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/.

326 I. Kouvakas, 'You Can't Have Your Apple and Eat It Too' (n 314).

327 IPA §255(8).

328 *Podchasov v Russia*, App no 33696/19 (ECtHR, 13 February 2024).

329 Ibid., para 77.

The Court held that Russia had *"overstepped any acceptable margin of appreciation"*[330] and that such measures *"impair the very essence of the right to respect for private life"* and couldn't be regarded as necessary in a democratic society.[331]

The lawfulness and secrecy of TCNs are currently being challenged,[332] but they remain a significant risk to human rights.

The privacy and security risks posed by TCNs only increase with the application of AI. For example, companies could be commanded to re-architect their systems to make bulk content or communications data available to the intelligence services. That data might not necessarily need to be ingested in intelligence systems but could be accessed using the powers surrounding third party bulk data sets. Companies might also be required to apply AI analysis to their systems, which they would not otherwise use, to facilitate intelligence access. And if TCNs aimed at creating backdoors in end-to-end encrypted systems are successful, those backdoors become even easier for malicious actors to access due to advancements in AI which facilitate finding and exploiting vulnerabilities.[333]

Bulk Surveillance: Authorising "Selectors"

Bulk interception permits the collection of large quantities of data, and it used to be difficult or impossible for intelligence agencies to examine it all.[334] To get around this resource constraint, they used *"simple selectors"* which act as a filter to ensure they only examine the most relevant material.

Selectors are the specific search term, identifiers, or rules that are used in the filtering process.[335] Selectors can be simple, for example, an email address of a

330 Ibid., para 80.

331 Ibid.

332 See Privacy International, 'PI Apple TCN Challenge', available at: https://privacyinternational.org/legal-action/pi-apple-tcn-challenge, accessed 10 September 2026.

333 See, e.g., AI Security Institute, Our Evaluation of Claude Mythos Preview's Cyber Capabilities, (13 April 2026) available at: https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities.

334 In the case of *Big Brother Watch and Others v The United Kingdom* 58170/13 62322/14 24960/15 which concerned bulk communications data, it was noted that "GCHQ did not have the capacity to read all communications" that it had intercepted (para 17). *Big Brother Watch v UK* (n 258).

335 Privacy International, How Bulk Interception Works' (n 83).

known target, or they can be broad, for example, all communication to or from a certain country.[336] Any communication that matches the selector is retained and examined, and all other data is typically (theoretically) deleted.[337]

Selectors accordingly determine the scope of the data that is seen and/or analysed, which has important consequences for the right to privacy. Their development and use can limit or expand the privacy intrusion.

Because of the important function of selectors, the European Court of Human Rights (ECtHR), in the matter of *Big Brother Watch and Others v The United Kingdom* (BBW), developed safeguards for their use.[338] Specifically, the ECtHR requires that the use of selectors, albeit only for targets within the United Kingdom, must be authorised. The Court acknowledges that it may be impractical to include every individual selector in a warrant application, but it should *"at the very least identify the types or categories of selectors to be used."*[339] Further, enhanced safeguards are required for *"strong selectors"*, or those linked to identifiable individuals. Strong selectors must be justified on grounds of necessity and proportionality, such justification must be recorded and subject to prior internal authorisation.[340] In addition, the selection and use of selectors, alongside all stages of the bulk interception process, must be subject to robust and continuous oversight by an independent authority to ensure the interference is limited to what is strictly necessary.[341]

While the explicit consideration and authorisation of selectors was an important innovation in the BBW judgment, the use of AI in the intelligence cycle has likely fundamentally changed the ways in which surveillance functions, which poses two concerns in the context of regulating selectors. First, the speed and capability of AI mean that intelligence agencies are unlikely to face the same capacity challenges – it is now possible for them to examine all of the bulk data that they collect. It is no longer necessary to only look at relevant data linked to a selector, because AI has

336 Ibid.

337 As identified in *Big Brother Watch and Others v United Kingdom* (n 258) see paras 15-19.

338 Ibid.,15-19.

339 Ibid., para 354.

340 Ibid., para 355.

341 Ibid., para 356.

the capacity to sift through it all. This is particularly significant where AI is used for pattern recognition, profiling or predictive analysis.

Instead of only examining relevant information flagged by a selector (e.g. people contacted by a certain telephone number that the intelligence agency has reason to believe is suspicious), AI reverse engineers the process, and analyses large quantities of data in order to flag who may be suspicious. If this is the use case, it is likely that all of the bulk data will be analysed, not just the data flagged by selectors. AI therefore reduces the practical importance of selectors as a safeguard because analysis may no longer be confined to data associated with pre-identified targets.

This fundamentally changes the level of intrusion and raises concerns about 'total'[342] or 'mass surveillance'[343] and power. These concerns are well articulated by legal scholar Neil M. Richards, Professor of Law at Washington University in St. Louis and one of the foremost experts in privacy law, who argues that total surveillance is illegitimate.[344] His remarks, made in 2013, well before the prevalence of AI, are even more pressing today:[345]

> *"The magnitude of technological change should not blind us to the important values that our law has protected for decades: the importance of private communications, intellectual privacy, and unfettered intellectual exploration. Moreover, a world of total surveillance would be one in which the power dangers of surveillance are even more menacing. In such a world, watchers would have increased power to blackmail, selectively prosecute, coerce, persuade and sort individuals. A world of total surveillance is not just science fiction. It is the world toward which we are slowly creeping, as software is coded, databases are combined, and each CCTV camera is successively added to the network."*

342 Editorial Board, 'Total Surveillance is Not What America Signed Up For' (The New York Times, 21 December 2019) available at: https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-privacy-rights.html.

343 See additionally Privacy International, 'Mass Surveillance', available at: https://privacyinternational.org/learn/mass-surveillance, for a further discussion on mass surveillance.

344 Neil M. Richards, 'The Dangers of Surveillance' (The Harvard Law Review Association, vol. 126, no. 7, 2013) available at: https://harvardlawreview.org/wp-content/uploads/2013/05/vol126_richards.pdf, pp. 1934–65.

345 Ibid.

The second challenge relates to the way AI analyses information. In BBW, the Court assumes that selectors are identifiable categories (e.g. keywords or identifiers) but AI does not work on such simple terms. Instead of looking for specific mentions of specific names, numbers, or dates, it identifies behavioural patterns, correlations, probabilistic models and engages in predictive profiling.[346]

It may be difficult, if not impossible, to distil these functions of AI into definable selectors for an authorisation process. Further, the internal reasoning of a model is not easily explainable (contributing to their description as *"black boxes"*),[347] which would make them hard to justify and record.

The use of AI in processing bulk data accordingly poses practical challenges for existing safeguards, raising concerns about what is currently restraining mass surveillance.

Examination warrants

Bulk interception and equipment interference warrants allow the UK intelligence agencies to collect bulk telecommunications data and content through interception and hacking. But the IPA limits how intelligence agencies use this data, by regulating the use of criteria for examination to identify material that is sent to, or intended for, an individual known to be in the UK.[348] However, the amount of data acquired through bulk interception[349] or hacking[350] is so vast that it will inevitably include information involving persons in the UK, and some information may not be overseas related at all. When an intelligence agency wants to examine information that is sent by or intended for someone in the UK obtained from a bulk interception or an equipment interference warrant, it must obtain a targeted examination warrant that more specifically identifies the target

346 Neli Sahota, 'Decoding the Mind: How AI Predicts Decisions Before They're Made' (Medium, 28 June 2025) available at: https://medium.com/@lisahota2019/decoding-the-mind-how-ai-predicts-decisions-before-theyre-made-d379a6864933.

347 See additionally, Jenna Burrell, 'How the machine 'thinks': Understanding Opacity in machine Learning Algorithms' (Big Data & Society, 2016) available at: https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512.

348 IPA pt 6, ch 1 §152; IPA pt 6, ch 3 §193.

349 Privacy International, 'How Bulk Interception Works' (n 83).

350 Privacy International, 'Government Hacking' (n 83).

of the warrant.[351] Targeted examination warrants are double-locked, and require a showing that granting the warrant, which involves the communications of persons in the UK, is necessary for a legitimate aim, and is proportionate to that goal.[352] However, the urgency carve-out (discussed above) also applies to them.[353]

Targeted examination warrants are only necessary for communications unrelated to people within the UK when seeking communications subject to journalistic or legal privilege.[354] For example, for seeking information subject to legal privilege, the warrant must exhibit *"exceptional and compelling circumstances"* that make it necessary to authorise the interception, the public interest in obtaining the information outweighs the public interest in the confidentiality of items subject to legal privilege, and there are no other means by which the information may reasonably be obtained.[355]

Above we discuss the limits of selectors in the age of AI enabled analysis – in short, they are simply not a practical means by which to regulate how intelligence agencies extract information from bulk personal datasets.[356] These limits interact with targeted examination warrants in two ways. First, if intelligence agencies are using AI in such a way that they no longer have to select what information to analyse, they very well may be analysing communications sent by or intended for people in the UK without necessarily satisfying the requirement that they *"know"* of their target's location, thus rendering the application of targeted examination warrants moot. Second, similarly threatened are the safeguards for legally and journalistic privileged material. It is likely that this material is being swept up in AI-enabled analysis of bulk datasets, and that new safeguards are required to protect associated fundamental rights.

351 IPA pt 2, ch 1 §15(3).

352 IPA pt 2, ch 1 §19(2). Specifically, the warrant must be necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the UK. §20(2)(c).

353 IPA pt 2, ch 1 §24.

354 IPA pt 2, ch 1 §§27-28.

355 IPA pt 2, ch 1 §27(4-6).

356 See n 333.

The National Security Exemption

The national security exemption is ubiquitous in UK laws, and the laws of most countries.[357] Broadly, it enables the state to withhold information or avoid compliance with certain legal obligations to protect state interests. While its purpose may be legitimate in some instances, it raises two significant concerns. First, the uncertain scope of national security enables scope creep and abuse, and second that the deference afforded to the executive on matters of national security undermines accountability mechanisms.

Scope creep

There is no fixed statutory definition of 'national security' in UK law.[358] None of the laws we examined included a definition of it or listed the kinds of activities it could encompass. Instead, the concept is primarily shaped by judicial precedent.[359] A definition of threats to national security was presented by the Interception of Communications Commissioner in the case of *Kennedy v UK*[360] as:

> *"activities which threaten the safety or well-being of the State and activities which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means."*

No objection to the definition was recorded in the judgment,[361] and it is considered a prevailing conceptualisation of national security.[362] But even this conceptualisation is vague – any number of activities could be said to threaten the safety or well-being of the State or undermine Parliamentary democracy. It could

357 See, e.g., the Promotion of Access to Information Act 2 of 2000 and the Protection of Personal Information Act 4 of 2013, which are South Africa's access to information and data protection laws, both of which contain national security exemptions.

358 Eric Metcalfe, 'Terror, reason and rights' in Esther D. Reed and Michael Dumper (eds);

Civil Liberties, National Security and Prospects for Consensus: Legal, Philosophical and Religious Perspective (CUP, 2012), David Feldman, 'Human rights, terrorism and risk: the roles of politicians and judges' (2006) PL, 364 – 384.

359 Central South University Human Rights Center, 'National Security and Human Rights' (Country Report, 2025) available at: https://www.hrug.legal/wp-content/uploads/2025/06/6.18-U.K.-final-report-.pdf page 2.

360 *Kennedy v United Kingdom*, App no 26839/05 (ECtHR, 18 May 2010), paras 33 & 159.

361 Daniella Lock, 'The protection of ECHR Rights in UK National Security Law' (UCL PhD thesis, 2022) available at: https://discovery.ucl.ac.uk/id/eprint/10168360/1/Daniella%20Lock%20Thesis%20Final%20Copy.pdf, p. 62.

362 Central South University Human Rights Center (n 358) p. 2.

include terrorism or the sabotage of critical infrastructure, but it could also be broad enough to be interpreted to include a lawful protest and political dissent.

The differing conception of its scope is highlighted by this 'definition' provided by the ICO. In a guide developed on the national security and defence exemption in the DPA, it was noted:[363]

> *"National security" is not specifically defined and can be interpreted in a flexible way to adapt to changing threats. [...] It is generally understood to cover the security and well-being of the UK as a whole, its population, and its institutions and system of government. For example, it can cover:*
>
> - *protection against specific threats, such as from terrorists or hostile states;*
> - *protection of potential targets even in the absence of specific threats; and;*
> - *international co-operation with other countries."*

The above definition builds in a degree of flexibility and appears to apply in the absence of specific threats. But other courts have found that national security concerns a particularly severe threat, and one which is present or foreseeable. In *La Quadrature du Net Commission v Poland* (LQdN)[364] the Court of Justice of the European Union considered national security to concern *"protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities."*[365]

363 Information Commissioner's Office, 'National Security and Defence Exemption: A Guide', available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide/#national-security, accessed 10 September 2026. Note: this guide does not apply to intelligence services or competent authorities processing for law enforcement purposes.

364 *La Quadrature du Net and Others v Premier ministre and Others* (Joined Cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

365 Ibid., para 135.

In the Court's view, the importance of safeguarding national security goes beyond other less significant objectives such as combatting crime (including serious crime), and even safeguarding public security. A threat to national security must be serious and *"shown to be genuine and present or foreseeable."*[366]

According to commentators, national security is *"distinguishable by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances."*[367]

The absence of a clear definition allows for expansive interpretation which could extend beyond strict security threats to broader state interests. This is particularly true considering the broad discretion given to individuals to determine whether a national security exemption should be applied. *"The possibility for states to invoke national security considerations to justify reductions in the protection which must be afforded to human rights is inevitably a source of concern, as the risk of abuse cannot be entirely ruled out."*[368] This could lead to unfair, inconsistent or arbitrary application of the law. National security and counter-terrorism laws have long been used, in the UK and abroad, as a pretence to unlawfully expand surveillance authority.[369]

Deference

In order to guard against the kinds of abuse and scope creep detailed above, the European Court of Human Rights has emphasised that the oversight of domestic surveillance regimes requires robust review of surveillance powers.[370] The UK developed its law in conformity with this and established

366 Ibid., para 137.

367 Plixavra Vogiatzoglou 'The AI Act National Security Exception',(Verfassungsblog, 9 December 2024) available at: https://verfassungsblog.de/the-ai-act-national-security-exception/.

368 European Court of Human Rights, 'National Security and European Case-law' (2013) available at: https://www.echr.coe.int/.

369 See, e.g., Privacy international, 'Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 Pandemic', (14 December 2022) available at: https://privacyinternational.org/report/5003/under-surveillance-misuse-technologies-emergency-responses-global-lessons-covid-19, see also: 'Politics of Digital Surveillance, National Security and Privacy' (Centre for Economics and Foreign Policy Studies, April 2018) available at: https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf.

370 Daniella Lock, 'The protection of ECHR Rights in UK National Security Law' (n 360) p. 245.

the Investigatory Powers Tribunal (IPT) in 2000.[371] The IPT is an independent judicial body[372] that has equipped judges with the powers to enable substantive, fact-finding scrutiny of national security measures, including assessing whether such powers have been used lawfully and in a manner that is necessary and proportionate.[373] The IPT adopts a quasi-inquisitorial process (as opposed to adversarial) and routinely uses closed proceedings.[374]

But despite these powers, research conducted by legal academic Daniella Lock found that judicial oversight in national security cases in the UK has degraded into a low-intensity standard of review, where courts only consider if a decision is irrational or unreasonable and not whether it is correct, justified or proportionate.[375] Specifically, she notes:[376]

> *"UK judges largely do not apply substantive, fact-finding scrutiny to surveillance powers and thus do not ensure such UK surveillance powers are only used when this is necessary and proportionate. This is due to the IPT largely replicating Strasbourg's approach to adjudication. This is in the form of its process-oriented and rationality review of domestic surveillance powers, which reflects the Court's particular institutional limitations as an regional court. The result of the IPT imitating Strasbourg is that there are gaps in the IPT's scrutiny, including of the substantive necessity and proportionality of general surveillance powers, and manner in which the SIAs [security and intelligence agencies] interpret their statutory powers in practice."*

Indeed, we see this approach in the European Court of Human Rights where states are *"recognised to have a certain – even a large – measure of discretion when evaluating threats to national security and when deciding how to combat*

371 Mria Theodoulou, 'Is the Investigatory Powers Tribunal Powerless?' (Computer Weekly, 30 April 2025) available at: https://www.computerweekly.com/opinion/Is-the-Investigatory-Powers-Tribunal-powerless.

372 For more on the IPT, see: https://investigatorypowerstribunal.org.uk/.

373 Daniella Lock, 'The protection of ECHR Rights in UK National Security Law' (n 360) p. 245.

374 Mria Theodoulou 'Is the Investigatory Powers Tribunal Powerless?' (n 370).

375 Daniella Lock, 'The protection of ECHR Rights in UK National Security Law' (n 360) p. 247.

376 Ibid., pp. 246 - 247.

these."[377] This means that although courts appear equipped to provide robust oversight, they rarely conduct full fact-based assessments of executive decisions, with the result that rights are not fully protected in practice. This dynamic contributes to the creation of what Lock describes as *"legal grey holes"*, in which safeguards exist in theory but operate weakly in reality. She notes:[378]

> *"despite extensive domestic institutional reform to enable substantive review of UK national security powers, including in appropriate contexts fact-finding and assessment of primary facts and evidence by judicial bodies, the manner that UK judges have applied their jurisdiction tends to dissolve into rationality review. As a result, UKNSL [United Kingdom National Security Law] is currently failing to protect fully ECHR [European Convention on Human Rights] rights, and the relevant UKNSL regimes have become 'legal grey holes' (LGHs) which are helping to normalize expanding executive national security power."*

Lock describes these legal grey holes (LGHs) as having three features:[379]

> *"First, there is a legal framework that contains some protections of the individual against the state. Secondly, these protections are insufficient for effectively challenging the executive's case. Thirdly, the legal regime gives the appearance of providing robust review and that the relevant national security powers comply with the rule of law, which affords the executive legitimacy while it exercises national security powers which are substantially under-reviewed."*

In effect, the appearance of robust review lends legitimacy to the exercise of national security powers, but in reality, the powers are under-scrutinised, allowing broad security powers to expand with only limited meaningful accountability. This is problematic in light of the safeguards and protections that national security exemptions circumvent.

377 European Court of Human Rights, 'National Security and European Case-law' (n 367) p. 2.

378 Daniella Lock, 'The protection of ECHR Rights in UK National Security Law' (n 360) p. 6.

379 Ibid., p. 84.

In the national security context, as it does in every other regulatory gap we discuss, AI only exacerbates a law's shortcomings. National security exemptions already made it incredibly easy for intelligence agencies to collect and analyse data without abiding by regulations and without needing to disclose what they were doing, all under the guise of serious legal review. AI allows agencies to do so more quickly, more effectively, with less scrutiny, and to more people – essentially allowing agencies to surveil the location, communication, relationships, internet activity (and more!) of whomever they wish. Although the traditional approach has been to defer to intelligence agencies in their application of national security exemptions, AI gives intelligence agencies so much power that it is essential that reform in national security contexts be taken up with the utmost urgency.

3. WHAT SHOULD BE DONE?

3.1 INTRODUCTION



As the above analysis sets out, the current UK investigatory powers regime has significant gaps when it comes to effective regulation of AI use by intelligence agencies. In the following section, we provide our recommendations for how this regulation could be improved, both by increasing the effectiveness of certain safeguards and drawing clear lines where AI should be prohibited, especially when it comes to automated decision making.

These recommendations use the UK investigatory powers legislation as a starting point, so are most applicable to the UK context. But they should also be generalisable to other jurisdictions. We strongly recommend they are implemented in primary legislation to guarantee necessary democratic control and oversight.

As an initial matter, we maintain our objection to generalised, or mass surveillance.[380] As discussed above, bulk data collected under mass surveillance powers is now likely central to much of the intelligence agencies' use of AI. This only heightens our concern that bulk surveillance puts entire populations under suspicion, as advancing AI tools are likely to make bulk data even more intelligible and the foundation for increasingly intrusive inferences. None of the recommendations below are meant to undermine our opposition to mass surveillance. They take the law in the UK as it is now, however, and so engage with warrantry regimes that permit bulk surveillance.

Although the UK investigatory powers regime regulates the collection of data, it neither clearly constrains nor provides oversight of any algorithms or software used to obtain or process said data and also fails to regulate relationships between government agencies and third-party software providers. This interaction between governments and third-party providers was demonstrated recently in

380 Privacy International, 'Fighting Mass Surveillance in the Post-Snowden Era' (20 December 2018) available at: https://privacyinternational.org/impact/fighting-mass-surveillance-post-snowden-era.

the controversy surrounding the US government's attempts to contract for AI services from companies Anthropic and OpenAI.[381] A core component of that controversy was the lack of rules in the US[382] to prevent human rights abuses through such arrangements. The UK system is no better. Our recommendations begin to try to address this gap, but there is much more to be done in order to effectively regulate these public-private partnerships.[383] The safeguards and limits recommended here may be stronger than those applied to commercial AI use, given the risks of abuses and human rights consequences of such abuses.

The recommendations are not meant to be exhaustive and, given the ever-changing nature of this technology, may soon benefit from further refinement. We welcome constructive feedback.

381 Privacy International, 'The Anthropic and US Government Conflict is Larger Than You Think' (27 February 2026) available at: https://privacyinternational.org/news-analysis/5739/anthropic-and-us-government-conflict-larger-you-think.

382 Faiza Patel, "AI and the Commercial Data Loophole' (n 39).

383 Privacy International, 'Safeguards for Public-Private Surveillance Partnerships', available at: https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships, accessed 10 September 2026.



3.2 PROHIBITED USES

We deem certain uses of AI by intelligence agencies to be so inherently incompatible with fundamental human rights standards that they should never be permitted, even with safeguards in place. These include:

- **Fully automated decision-making**: taking a decision based solely on automated processing which has legal or significant effects on an individual, including determining the target(s) of surveillance or any other government action;
- **Sentiment analysis**: detecting, measuring or inferring a person's emotional state;
- **Behavioural prediction**: predicting the likelihood a person will be a threat to national security based solely on AI profiling or assessing their personality traits and characteristics;
- **Profiling based solely on protected activities**: profiling, targeting or tracking a person based solely on their exercise of their human rights, including freedom of expression, assembly, opinion and religion;
- **Disadvantaging or profiling a person based solely on protected characteristics**: disadvantaging or profiling based solely on ethnicity, national origin, race, sex, gender, sex life or sexual orientation, political opinions, trade union membership, religious or philosophical beliefs;
- **"Live" identification of a person based on biometrics**: real-time remote biometric identification of a person;
- **Scraping to create biometrics databases**: use of AI to create or expand biometrics databases through the untargeted scraping of biometrics from the internet or CCTV footage;
- **Relying solely on AI for analysis**: using AI as the only means of producing an intelligence analysis;

- **Forcing third-party AI use**: requiring third parties to apply AI to their systems for the purpose of facilitating intelligence analysis; and
- **AI-directed equipment interference**: relying solely on AI without human oversight to detect and exploit vulnerabilities that may allow access to systems or devices.

When we use the word "solely" in the prohibition on automated decision making, we intend it to encompass scenarios not only where the AI makes and actions a decision on its own, but also where a human may be required to implement the decision but does not substantially engage with the decision-making process.

In other words, "rubber-stamping" of AI-based decisions should also be prohibited. Any decision taken based on AI analysis should have meaningful human involvement.[384] This is an especially important clarification in the intelligence context as objects of such decisions will have much less transparency about them and often little practical ability to challenge them.

These prohibitions are roughly aligned with uses which are prohibited or significantly restricted in other prominent AI policies, including the EU AI Act and the October 2024 US National Security Memorandum on AI[385] which was since rescinded by the Trump administration.[386] They also reflect the consensus of the international community (including UN General Assembly Resolutions A/RES/78/265 and A/RES/80/215) and independent international human rights experts such as the UN Special Rapporteur on counter-terrorism and human rights.[387]

There are likely other uses of AI which should not be permitted.
We would welcome constructive feedback on this list.

384 Ben Green, 'The Flaws of Policies Requiring Human Oversight of Government Algorithms', Computer Law & Society Vol.45, available at: https://www.sciencedirect.com/science/article/pii/S0267364922000292.

385 The White House, 'National Security Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence (NSM-25)' (GovInfo, 24 October 2024), available at: https://www.govinfo.gov/content/pkg/DCPD-202400945/pdf/DCPD-202400945.pdf.

386 Presidential Memorandum, 'National Security Presidential Memorandum/NSPM-11 (5 June 2026) available at: https://www.whitehouse.gov/presidential-actions/2026/06/national-security-presidential-memorandum-nspm-11/.

387 United Nations Office of the High Commissioner, 'Protecting Human Rights While Using Artificial Intelligence to Counter Terrorism' (15 December 2025) available at: https://www.ohchr.org/en/documents/position-papers/protecting-human-rights-while-using-artificial-intelligence-counter.

3.3 STAGE 1 – DATA COLLECTION

Principles applicable to all warrants and authorisations

Where an AI is used in obtaining a warrant or authorisation, or will be used in the conduct authorised, the warrant or authorisation application should:

- state whether AI was or will be used at any stage of the application or investigative process;
- reveal the purpose of the AI used or to be used and its capacity and limitations in carrying out that purpose (e.g. to identify surveillance targets, to interpret content of communications, to assess risk, to conduct an internal assessment regarding impact on rights);
    - An overview of the AI system's design should also be given including what sort of management decisions are made by the algorithm (and whether they are advisory or decisive); whether the algorithm relies on neural networks, machine learning, probabilistic functions or other types of logic; what training data was used; and under what circumstances the algorithm is not deployed or has a failsafe.
- explain why the use of AI is necessary for the purpose(s) stated, and why less intrusive methods could not achieve the objective;
- describe in detail the source and assessed accuracy of inputs for the AI system (e.g. what data was or will be obtained or used);
- identify risks of the use of AI particular to the warrant or authorisation, which could include inaccuracy, bias, processing sensitive data, and others, with specifics as to any data or model used and their accuracy thresholds, as well as what mitigations are or will be applied to limit these risks;
- explain how data used for any AI analysis was or will be minimised to what is strictly necessary.

- This explanation should explicitly include any guardrails incorporated into the AI to limit its use to what is necessary and proportionate.
- The guardrails should include, but are not limited to, limiting the analysis to approved data sources, and requiring necessary levels of transparency when providing responses or recommendations (e.g. what reasoning must be presented and evidence cited by the system).
- The authorising authority should be able to interrogate and change these required guardrails prior to any authorisation being approved.

The Judicial Commissioner or other independent authorising authority should interrogate all of this information in deciding whether to approve the warrant or authorisation.

In the case of any renewal applications, this information should be updated and re-interrogated, especially given the rapid advancement of AI.

Targeted Warrants and Authorisations

Where AI will be used to facilitate the execution or application of a targeted warrant, such as for targeted interception or equipment interference, in addition to the general requirements above, the warrant should identify and justify based on reasonable suspicion, necessity and proportionality:

- the relevant criteria for examination, which may include, but are not limited to:
  - any search terms or selectors to be applied through the system;
  - any prompts to be used; and
  - any other way in which the system will be directed to process or analyse the information the warrant seeks.

Bulk Warrants

With regard to bulk warrants, a presumption should be applied that advanced AI will be used to process the bulk data and therefore all of the above general safeguards must be complied with.

Given the substantial increase in the intrusiveness of bulk surveillance when it is facilitated by AI, a bulk warrant should only be authorised if it is strictly necessary within the meaning of strict necessity as developed by the European Court of Human Rights in *Big Brother Watch and others v UK* and subsequent case law. Some bulk warrants, especially those that may capture or reveal sensitive biometric data, may never be deemed proportionate in light of *S and Marper v the United Kingdom*[388] and similar case law.

Using AI for the targeted examination of any material (including content, communications data, bulk personal datasets) obtained using a bulk warrant must be authorised by an examination warrant with the safeguards detailed below.

388 *S and Marper v United Kingdom* [GC], Apps nos 30562/04 and 30566/04 (ECtHR, 4 December 2008).

Problematic Collection Outside of the Warranty Process

As we identify in our analysis (section 2.3) there are several provisions in the UK investigatory powers regime which allow intelligence agencies to access data prior to obtaining a warrant or authorisation. This pre-authorisation access is mainly justified on the basis of urgency or low risk of significant privacy intrusion. But AI makes these pre-authorisation uses of data potentially much more intrusive, and harder to rollback if authorising bodies later decide that the pre-authorisation use was unjustified.

For these reasons, we suggest the following amendments to these regimes:

- Urgency carve-outs
    - There should be mandatory deletion of any information collected or reviewed, including deletion of any subsequent intelligence generated, if the warrant or authorisation sought after the urgency period is denied. This removes discretion currently permitted with regard to deletion.
    - Data acquired on the basis of urgency should not be incorporated into any AI system or training dataset until the post-urgency warrant or authorisation is obtained.
    - Records should be kept of how many times each agency relies on urgency, and if that number passes an identified threshold for pre-AI urgency reliance, it should trigger an investigation by the IPCO.
    - The IPCO should update its public reporting to include how many warrants were issued under urgency and subsequently refused by a Judicial Commissioner.
- Assessing third-party Bulk Personal Datasets (BPDs) (section 2.3)

- Specify what "assessment of value" includes for third-party datasets, and explicitly prohibit some use cases during the assessment phase such as individual targeting, profiling, predictive analysis, and using inspection data to train AI models.
- Include quantity thresholds for the assessment of third-party datasets which would set the max volume of data that can be analysed or number of records accessed during the assessment.
- Prevent intelligence agencies from ingesting a third-party dataset into their own systems during assessment to prevent ingestion of such data into internal AI systems.
- After the value assessment, require mandatory deletion of intelligence agency internal copies of data analysed and any outputs of the third-party dataset if authorisation is not subsequently applied for and granted.

We also advocate for the complete removal of the recently added concept of low or no privacy datasets, as explained in our analysis (section 2.3).

In short, we recommend:

- Low/no privacy datasets
  - Remove the option to obtain low/no privacy datasets under a lesser authorisation regime as the inferential power of AI means almost all data may now form the basis for intrusive inferences, especially when combined with other large datasets.

3.4 STAGE 2 – MAKING THE DATA USEABLE

Combining Data

Combining data or datasets obtained under the aforementioned warrants for the purposes of AI analysis raise a new set of concerns. The combination may increase the intrusive capacity of analyses, including facilitating de-anonymisation and inference, and can amplify biases in related datasets, among other things.

Therefore, a separate authorisation should be obtained before data collected under any of the investigatory powers - targeted or bulk - is combined for further analysis by AI.

That authorisation should:

- describe which data will be combined;
- declare the purpose pursued through the combination;
- explain why it is necessary and proportionate to combine the data for that purpose;
- describe the AI to be applied to the data, including its capacities and limitations;
- identify any new risks, such as increased inaccuracy, bias or intrusive inferences, which may arise from the application of AI to the combined data, and the mitigation measures to be adopted; and
- assess and provide assurance that the data is adequate, relevant, accurate and up to date before combination.

Data obtained through urgency processes, as discussed above, should never be combined until full post-urgency authorisation is granted.

Agencies should also retain the possibility to 'undo' combinations of datasets and updates to models based on those combinations, such as by keeping previous versions which can be restored. Further, when

data is deleted following the expiration of the data retention time limit, or for any other reason, such deletion should be reflected in any combinations of datasets and any subsequent intelligence generated.

If agenticAI is used on combined datasets, it must be clearly limited by the scope of the combination authorisation.

The agenticAI must:

- be constrained by guardrails limiting the datasets it has access to, and not allowing it to discover its own datasets, especially outside of the confines of the combinations permitted by the authorisation;
- record the datasets accessed and data combined in its analysis; and
- not be allowed to search for data outside of the authorised datasets, including from sources outside of agency control.

AgenticAI

The use of AgenticAI has been deemed a *"qualitative step change"* by the UN.[389] Undoubtedly, further safeguards will be necessary to deal with the challenges of control, oversight and governance posed by agenticAI, but those are beyond the scope of this paper.

389 Preliminary Report of the Independent International Scientific Panel on AI, (n 9) §6.2.

3.5 STAGE 3 – USING THE DATA

Examination

The UK IPA currently requires the intelligence agencies to obtain additional *"examination warrants"* for certain more targeted searching of bulk data obtained under the bulk powers. We propose the following changes to examination warrants in order to better protect against increasingly powerful AI analysis.

- Where an AI system will be used to facilitate targeted examination, the warrant should include:
    - an identification of and justification based on reasonable suspicion, necessity and proportionality for the relevant criteria for examination, which may include, but are not limited to:
        - any search terms or selectors to be applied through the system;
        - any prompts to be used; and
        - any other way in which the system will be directed to process or analyse the information the warrant seeks; and
    - a description of the intended output(s) of the examination, including identification of key underlying parameters/profiles that underpin any output(s); and
    - if the purpose, or one of the purposes, of the examination is to identify any items subject to legal privilege or journalistic privilege, then heightened safeguards must apply, including that there are exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria.
- Examination warrants should also be required under a wider set of circumstances, including:

- any targeted examination of bulk data is undertaken, not just for "an individual known to be in the British Islands" at the time of selection for examination; and
- whether the targeted examination is of intercepted content, material obtained by equipment interference, communications data or bulk personal data.

This increased application of examination warrants acknowledges the seed change in the power of AI analysis. Under the current UK IPA, examination warrants are only required when *"any criteria used for the selection of the intercepted content for examination are referable to an individual known to be in the British Islands at that time."*[390] That safeguard was, in our opinion, always too limited, but becomes essentially useless with the application of modern AI as where previously it might have been possible to know a particular selector used to search bulk data was *"referable to an individual known to be in the British Islands"*, modern AI makes it easy to claim ignorance. Instead of using a specific selector such as a British phone number, an intelligence analyst can now enter a natural language prompt such as *"identify anyone who may be planning an attack on London"*. While that prompt might return British-based individuals, it is technically location neutral as to the target of the search, so might evade an examination warrant. Removing the limitation of requiring examination warrants only for searches *"referable to an individual known to be in the British Islands"* will close this loophole.

390 IPA section 152(4).

Logging, Audits and Transparency

Modern AI systems are notoriously opaque (see section 1.3 above) and can return inaccuracies, hallucinations[391] and even intentional deception.[392] Transparency is thus key to assessing and relying on the results of AI-facilitated analysis, as well as permitting effective internal and external oversight.

We recommend that records be kept with the following information to allow assessment and auditing of AI-generated outputs:

- audit trails for when AI has been used and what for (including when used for upstream analysis or profiling on which later decisions are based);
- assessments of the accuracy and potential bias of any data inputted into an AI system;
- impact assessments that cover the full range of rights, accuracy, and biases implicated by the application of AI (done afresh for each combination of datasets/models/prompts);
- human reviewable reasons for outputs, including verifiable data sources, logic, parameters and assumptions used;
- systems should incorporate "chain of thought" mechanisms whereby the model outlines its reasoning steps before answering; and
- post-analysis monitoring should include records of assessment of anonymized, aggregated AI usage patterns, of the accuracy of inferred data, and of bias, and interrogation and follow up on error reporting.

Some of the above information should have already been assessed and captured in the authorisation processes recommended above, but we repeat it here to emphasise the need to maintain and continually audit such information. The goal is to ensure that intelligence operators and oversight mechanisms can

391 Preliminary Report of the Independent International Scientific Panel on AI, (n 9) p. 34.

392 United Nations, 'Brief of the Scientific Advisory Board on: AI Deception', 19 March 2026, available at: https://www.un.org/scientific-advisory-board/en/ai-deception.

adequately understand and interrogate the functioning of algorithmic processes and their outputs, as well as the sources and weighting of underlying datasets.[393]

There must also be unambiguous human and institutional accountability for decisions taken as a result of AI analysis, especially when agentic tools are used. As emphasised in the EU AI Act, human reviewers must have the information necessary to *"remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons."*[394]

Training Data

The IPA explicitly allows for acquisition of data for *"testing or training activities"*[395] (see, e.g., section 17(2)(c)). The training of AI models is a vast topic that is outside the scope of these recommendations. But further consideration should be given to increased scrutiny and safeguards for this training given its increased importance to modern AI systems.

Oversight and Redress

Effective oversight from a body independent of the intelligence agencies is key. In the UK, the Investigatory Powers Commissioner's Office (IPCO) and the Information Commissioner's Office (ICO) should both have a role in this oversight. In order to do so, however, they need to be sufficiently resourced and have access to the necessary technical expertise to interrogate increasingly complex AI systems.

These oversight bodies should have the following powers and obligations:

393 See United Nations Special Rapporteur on the promotion and protection of Human Rights and Fundamental Freedoms while Countering Terrorism, 'Protecting Human Rights While Using Artificial Intelligence to Counter Terrorism' (December 2025) available at: https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/un-sr-ct-ai-position-paper-dec-2025.pdf.

394 EU AI Act, art. 14(4)(b).

395 See IPA §17(2)(c).

- the power to assess, then approve or reject AI systems the agencies propose to use prior to their deployment. This power would exist independently of the warrantry and authorisation powers discussed above which mainly focus on the acquisition and use of data, not technical systems;
- the entitlement to receive regular reports with details of all AI systems in use, and assess their continuing necessity;
- access to all records of AI systems, including logs and audit trails described above, as well as the ability to demand more granular information if needed;
- the ability to carry out bias and error testing and algorithmic audits of any AI system;
- the power to re-run models independently, including running searches and entering prompts;
- the power to inspect training datasets;
- the obligation to undertake enhanced assessment of any use of agenticAI, to address issues such as alignment faking, scheming to achieve uncontrolled goals, and evaluation awareness; and
- the obligation to regularly re-examine whether datasets acquired under warrants or authorisations are still appropriate for the purposes set out.

Our analysis (see section 2.2) demonstrates how easily data protection authorities, such as the ICO, can be excluded from oversight in the national security context. To help remedy this, we recommend conducting a review of the scope and effectiveness of the ICO's oversight role in relation to intelligence agencies data processing activities, with particular attention to the breadth and operation of exemptions and exclusions that limit that role. The review should assess whether current frameworks allow significant aspects of intelligence agencies' use of personal data to fall outside meaningful independent scrutiny, and what additional safeguards are needed to enable effective oversight.

Finally, transparency to facilitate redress is often elusive in the national security context but should be incorporated into an effective AI oversight regime. It should include:

- Annual reports from relevant regulators revealing as much as possible about AI use; and
- Notification to individuals affected by AI-facilitated decisions, where practicable, unless a delay in notification is independently authorised in strictly limited circumstances, such as where notification would seriously jeopardize the purpose for which the surveillance is authorised, or where there is an imminent threat to human life.

3.6 NATIONAL SECURITY EXEMPTIONS FROM DATA PROTECTION REQUIREMENTS

The above recommendations are designed to apply to intelligence agency use of AI. We presume the intelligence agencies will most often be acting to protect national security, and thus, national security is not a reason to exempt them from any of the above proposals. Indeed, the UK Investigatory Powers Act explicitly regulates and brings national security activities within scope.

As discussed throughout this paper (see sections 2.2 and 2.3) however, many current legal regimes that could apply to intelligence agency use of AI, such as data protection law, have significant and poorly defined national security exemptions. For instance, the UK government can issue national security certificates to exempt from data protection requirements a wide range of government bodies acting in the interest of national security.

These blanket exemptions are no longer tenable in the age of AI and its increased capacity for intrusiveness. As the European Court of Human Rights declared in *Klass and other v Germany*, *"[i]n view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse."*[396] Thus, even secret surveillance designed to protect national security is not fully exempt from regulation.

We recommend removing blanket national security exemptions in their entirety from data protection frameworks. Instead, narrower exemptions could be promulgated in a fashion more similar to what has been proposed in the EU AI Act (although we do not fully agree with the scope of those exemptions, either).

While broader exemptions continue to exist, we propose the following recommendations as a way to begin to narrow them to increase accountability and better protect against abuse.

396 *Klass and Others v Germany*, App no 5029/71 (ECtHR, 6 September 1978), para 50.

- "National security" must be more narrowly defined when it is the foundation of an exemption. Most current exemptions use the term with little attempt to define it, leading to potential for significant overuse and abuse, especially when the exemption will often be applied in secret. Definitions of aspects of national security, such as terrorism have been attempted and should be consulted.[397]
- Any certificate-based exemption, such as permitted under UK law to exempt the intelligence services from data protection requirements, must be:
    - mandatory, such that the exemption cannot be engaged unless a certificate is issued prior to the exemption being claimed: and
    - limited to 6 months in duration, and then it must be re-issued or renewed.
- The authority who would normally oversee the powers being exempted (for example, the UK ICO), must receive:
    - confidential notification of the certificate of exemption; and
    - the ability to audit and challenge the certificate of exemption.
- There shall be annual, public reporting on the number of certificates granted and rejected.
- People affected by an exemption should be notified once a certificate expires or is not renewed.
- Certificates should be challengeable in the Investigatory Powers Tribunal, either on assumed facts or post-notification.

397 United Nations General Assembly, 'Defining Terrorism to Respect and Protect Human Rights', A/HRC/61/52 (8 January 2026), available at: https://docs.un.org/en/A/HRC/61/52.

CONCLUSION

The UK's patchwork of existing laws goes some way in regulating the AI pipeline, but it is fragmented, uncertain and full of gaps. In our view, it is not enough.

Intelligence agencies are using AI. But while the UK's regulatory framework enables their capabilities, it doesn't effectively mitigate AI's risks. The presence of broad national security exemptions weakens the effectiveness of existing safeguards. These exemptions allow intelligence agencies to bypass key protections in data protection, human rights and equality law. Sector-specific legislation, like the IPA, fails to provide sufficient safeguards to restrict the increasing power of AI. At the same time, oversight mechanisms themselves are constrained, tending towards deferential review and potentially leaving important decisions, possibly made with AI, insufficiently scrutinised.

Taken together, the current framework appears to enable the expansion of AI surveillance without proportionate safeguards. As AI continues to shape data use and intelligence practices, there is a growing need for a more coherent and explicit regulatory approach – one that meaningfully addresses AI-specific risks.

APPENDIX 1 : THE AI PIPELINE & USE CASES

Stage 1: Data Collection		
Data source	**Relevant Legislation**	**Authorisation mechanism**
Bulk personal data (BPD) This would include large datasets with personal data about a large number of people the majority of whom are unlikely to be threats to national security. Examples may include: electoral rolls, passport records, social media activity, travel records, and financial records.	Part 7of the Investigatory Powers Act 2016 (IPA): Standard BPD	Double-lock: Warrant issued by Secretary of State, approved by Judicial Commissioner
	Part 7A of the IPA: Datasets with no/low expectation of privacy	Head of agency grants authorisation, approved by Judicial Commissioner
	Part 7B of the IPA: Third-party BPD	Double-lock: Warrant issued by Secretary of State, approved by Judicial Commissioner
Bulk personal data held by a third party (Third-party BPD) This refers to bulk person datasets held by third parties. Intelligence agencies typically look at it on the third parties' system. But there is a loophole in the law that lets them have a quick look at it without a warrant to determine if it is useful, during this 'quick look' they can assess it on their own system.	Part 7B of the IPA: Third-party BPD	Double-lock: Warrant issued by Secretary of State, approved by Judicial Commissioner
Bulk communications data (BCD) These are also bulk data sets, but they only include details about the 'who', 'when', 'how' and 'with whom' of communications, often referred to as metadata. They may also include IP addresses, types of devices, network connections, search histories and location data. The content of emails, messages and calls will be excluded. This data is obtained from telecommunications operators, such as phone companies and online platforms.	Part 6, Chapter 2 of the IPA	Double-lock: Warrant issued by Secretary of State, approved by Judicial Commissioner

Stage 1: Data Collection		
Data source	**Relevant Legislation**	**Authorisation mechanism**
Targeted communications data This is the same information as described in bulk communications data, above, but it does not relate to a large group of people – it relates only to one or a few people.	Part 3 of the IPA	IPCO authorisation / Self-authorisation: Authorised by IPCO or a senior officer in the agency.
Intercepted Communications (Targeted and Bulk) This is the content of communications (phone calls, emails, letters, messages). It can be intercepted while in transit (when it is being communicated over a network) or collected from storage (such as a hard drive or cloud storage).	For targeted interception – Part 2 For bulk interception – Part 6, Chapter 1	Double-lock: Warrant issued by Secretary of State, approved by Judicial Commissioner
CCTV/Surveillance This is everything captured through a CCTV camera, which can be public or privately owned. It could include: facial images, gait, body language, movement across public spaces, traffic flows, time and locations stamps.	Section 28 of the Regulation of Investigatory Powers Act 2000 (RIPA): Directed surveillance	Authorised by a designated internal officer and approved by a judicial authority.
	Section 32 of RIPA: Intrusive surveillance	Prior approval by the Secretary of State or senior authorising officer
Open-source intelligence This could include public records (e.g. government databases that are published, such as business records), media, academic content and potentially anything publicly available.	Likely part 7A of the IPA: Datasets with no/low expectation of privacy[1]	Head of agency grants authorisation, approved by Judicial Commissioner
	If conducted regularly, it may amount to directed surveillance in terms of section 28 of RIPA	Authorised by a designated internal officer and approved by a judicial authority.

1 We don't think open-source content should be categorised as datasets with low/no expectation of privacy but anticipate the government will do so. See for example, this article that includes "content from video-sharing platforms" as an example of the type of information that could be included: Harry Davies, The Guardian, 'UK Spy Agencies Want to Relax 'burdensome' Laws on AI Data Use, 2023, available here: https://www.theguardian.com/technology/2023/aug/01/uk-intelligence-spy-agencies-relax-burdensome-laws-ai-data-bpds.

Stage 1: Data Collection		
Data source	**Relevant Legislation**	**Authorisation mechanism**
Social media intelligence Content posted on social media, including likes, followers, photos, video, user reactions etc.	Likely part 7A of the IPA: Datasets with no/ low expectation of privacy[2]	Head of agency grants authorisation, approved by Judicial Commissioner
	If conducted regularly, it may amount to directed surveillance in terms of section 28 of RIPA.	Authorised by a designated internal officer and approved by a judicial authority.
	If an agent creates a fake profile to gain private access, it may amount to covert human intelligence under section 32A of RIPA.	Authorised by a designated internal officer and approved by a judicial authority.
2 We also don't think content on social media should be categorized as datasets with low/no expectation of privacy but anticipate the government will do so. See for example, this article that includes "content from video-sharing platforms" as an example of the type of information that could be included: Harry Davies, The Guardian, 'UK Spy Agencies Want to Relax 'burdensome' Laws on AI Data Use, 2023, available here: https://www.theguardian.com/technology/2023/aug/01/uk-intelligence-spy-agencies-relax-burdensome-laws-ai-data-bpds.		
Electronic data protected by encryption This includes data protected by encryption – on a device, on the cloud, or in transit. Mathematical algorithms protect the encrypted data while in transit or storage, allowing only the sender and intended recipients to access it. Data protected by encryption may include financial details, personal information and private messages.	If hacking, Part 5 of the IPA: Equipment interference Or bulk equipment interference (Part 6)	Double-lock: warrant issued by the Secretary of State and approved by a Judicial Commissioner.
	If compelled, Part 9, section 253 of the IPA: Technical Capability Notice	Double-lock: granted by the Secretary of State and approved by a Judicial Commissioner.
	If requesting encryption key, section 49 of RIPA	Written permission to give a section 49 notice must be granted by a Circuit Judge (in England and Wales), A Sheriff (in Scotland) or a country court judge (in Northern Ireland).

Stage 1: Data Collection		
Data source	**Relevant Legislation**	**Authorisation mechanism**
Internet of things data This is data collected by everyday objects that are connected to the internet and include: doorbell cameras, robot vacuums, smart watches, baby monitors, smart electricity meters etc.	If accessing device, then equipment interference under Part 5 of the IPA	Double-lock: warrant issued by the Secretary of State and approved by a Judicial Commissioner
	If accessing it through a cloud controlled by a third party, then Part 7B of the IPA	Double-lock: warrant issued by the Secretary of State and approved by a Judicial Commissioner
Privileged data received from other countries This is typically shared between law enforcement around the world, the receipt of which could be solicited or unsolicited. The collection of it would be governed by the sender's laws.	Constructive warrant: section 9 of the IPA prohibits a request being made unless a targeted interception or examination warrant under Part 2 has been issued.	Double-lock: warrant issued by the Secretary of State and approved by a Judicial Commissioner
Hacked data This includes the same kinds of data detailed above (e.g. communications) but it is acquired in a different way – by hacking a device. In this context, intelligence agencies don't obtain permission or assistance from the end-user or an intermediary company, they hack directly into a device to obtain the data.	For a single person - targeted equipment interference warrant – Part 5 If its bulk – bulk equipment interference data – Part 6, Chapter 3	Double-lock: warrant issued by the Secretary of State and approved by a Judicial Commissioner

Stage 2: Making the Data Useable
Data Preprocessing What is it and how is AI used in this process? Raw data is cleaned, standardised, transformed into a useable format for AI models, and labelled[3] Some of which entails removing duplicates, correcting errors, and normalising formats. AI can be used during this process. For example, natural language processing could be used to interpret names and contact information and machine learning models could be used to compare records to determine and remove any duplication[4]. Synthetic data could be created at this stage, for example, generative models could be used to create plausible values based on existing patterns to fill gaps.
Data Integration What is it and how is AI used in this process? Data from multiple sources is combined into a single data set which can include structured and unstructured data.[5] For example, Palantir has developed an Investigative Case Management System that combines disparate streams of data into a single investigative platform which allows agents in the USA to search multiple streams of data in one place.[6]

3 Prompt Panda, 'Elevate Your AI Game: The Key to Successful Prompt Preprocessing', available at: https://www.promptpanda.io/blog/ai-prompt-preprocessing/.

4 Ian Ormesher, 'Duplicate Detection with GenAI' (1 July 2024), available at: https://medium.com/data-science/duplicate-detection-with-genai-ba2b4f7845e7.

5 IBM, 'Structured vs. Unstructured Data: What's the difference?', available at: https://www.ibm.com/think/topics/structured-vs-unstructured-data

6 Caroline Haskins, Wired, 'ICE is Paying Palantir $30 Million to Build 'ImmigrationOS' Surveillance Platform', (18 April 2025), available at: https://www.wired.com/story/ice-palantir-immigrationos/

Stage 3: Using the Data	
3.1 using the data for training	
Use in the UK	Training
Intelligence agencies and other government bodies in the UK could use numerous sources of data, including bulk personal datasets, to train AI models. [7]	Data may be used to teach AI models to make accurate predictions. Data may be similar to the types described above or it could be generated (called synthetic data) for the purpose of training. [8] Data is fed into AI algorithms which have been developed to learn in specific ways. There are three broad ways of doing this, though they can also be combined: Supervised learning: the model learns from labelled examples. The training data has the correct label attached, the AI reviews it, learns the patterns or features, confirms if its correct and adjusts. For example, if it is learning to identify a human face, it will be given data labelled 'face' or 'not face'. The model learns to associate face-relevant features with the label 'face'. This allows it to identify a face when presented with new, unseen data. [9] Unsupervised learning: the model is given data without any labels or correct answers, and it has to find patterns, trends, anomalies or structure on its own. It is more exploratory and is typically used to identify hidden patterns or structures in data that may be unknown. [10] Reinforcement learning: the model learns by trial and error and is guided by rewards and penalties. Instead of being shown the correct answers, the AI takes actions in an environment and is given feedback – a reward or punishment. This helps it to understand the consequences of its actions (good or bad) and it learns to make better decisions. Common examples of this are models that learnt to play games, and they adjust their strategy based on the feedback – winning or losing. [11]

7 Davis Anderson, 'Independent Review of the Investigatory Powers Act 2016', (June 2023), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1166726/Independent_Review_of_the_Investigatory_Powers_Act_2016-FINAL.pdf.

8 Nayna Jaen 'How AI is Trained: The Critical Role of AI Training Data' (26 March 2024), available at: https://www.rws.com/artificial-intelligence/train-ai-data-services/blog/how-ai-is-trained-the-critical-role-of-ai-training-data/

9 Ibid.

10 Ibid.

11 Ibid.

3.2 Using the data for analysis for operational purposes		
Identity verification		
Police and intelligence agencies could use AI-enabled live facial recognition[12] in the UK.	Facial Recognition	Data Protection Act 2018: there is a broad national security exemption which allows non-compliance with the following: the data protection principles (except it must be lawful); data subject rights; communicating a data breach; some of the functions and powers of the Information Commissioner (including powers of entry and inspection). Importantly, they may not need to comply with the right not to be subjected to automated decision-making, the right to intervene in automated decision-making and the right to information about decision-making. The Human Rights Act 1998: the following convention rights may be limited for the purpose of national security, but still require substantive restrictions on any violation of the right: the right to a fair trial (only to the extent concerning the public's access to trial) (Art.6); the right to respect for private and family life (Art.8); Freedom of expression (Art.10), and Freedom of Assembly and association (Art.11). The Equality Act 2010: Includes a broad exemption for national security (Section 192) which states that a person doesn't contravene the Equality Act by doing anything it is proportionate to do for the purpose of safeguarding national security

12 Robert Booth, The Guardian, 'How Does Live Facial Recognition Work and How Many UK Police Forces Use It?', 93 May 2026), available at: https://www.theguardian.com/technology/ng-interactive/2026/may/03/how-does-live-facial-recognition-work-and-how-many-uk-police-forces-use-it.

3.2 Using the data for analysis for operational purposes		
Identity verification		
The banking, government services, and healthcare sectors all use[13] AI enabled voice analysis for identification. It is likely that intelligence agencies have access to similar technologies.	Voice analysis	Data Protection Act 2018 (same as above) The Human Rights Act 1998 (same as above) The Equality Act 2010 (same as above)
Intelligence agencies in the UK likely use AI powered gait analysis systems like NEC's BioIDiom[14] in conjunction with CCTV footage to identify suspects.	Gait Analysis	Data Protection Act 2018 (same as above) The Human Rights Act 1998 (same as above) The Equality Act 2010 (same as above)

13 Hannah-Rose Shearman, 'When Voice is No Longer Proof: AI Vocal Cloning and The Limits of Voice-Based Authentication', (2 March 2026), available at: https://bisi.org.uk/reports/when-voice-is-no-longer-proof-ai-vocal-cloning-and-the-limits-of-voice-based-authentication.

14 NEC, 'Commitment to Biometric NEC is Promoting Bio-IDiom – NEC's Biometric Authentication Brand', available at: https://www.nec.com/en/global/techrep/journal/g18/n02/180203.html.

Assessment		
The Ministry of Justice in the UK uses an AI powered risk assessment tool[15] to "predict" the risk of re-offending of thousands of people in prison and on probation every week. Some law enforcement bodies in the UK use AI to predict if individuals are likely to commit crimes,[16] with a view of nationalising these systems. Intelligence agencies also likely use this technology, but we do not have confirmation of their use.	Individual Risk Assessment	Data Protection Act 2018 (same as above) The Human Rights Act 1998 (same as above) The Equality Act 2010 (same as above)
UK intelligence agencies likely use sentiment analysis[17] tools similar to Babel and Shadow Dragon to analyse human behaviour from data. MI5 admits it is "increasingly making use of artificial intelligence to support" its analysis.[18]	Sentiment Analysis	Data Protection Act 2018 (same as above) The Human Rights Act 1998 (same as above) The Equality Act 2010 (same as above)
UKRI is currently funding an AI powered map[19] for use by law enforcement that identifies where crime is concentrating, and where it is likely to occur. UK intelligence agencies are likely using software like Palantir's ELITE software,[20] that Immigration and Customs Enforcement in the US is reportedly using to map targets for deportation.	Predictive mapping	Data Protection Act 2018 (same as above) The Human Rights Act 1998 (same as above) The Equality Act 2010 (same as above)
UK intelligence agencies likely use AI powered software similar to predictive policing software[21] to analyse past and predict future behaviours.	Profiling (behavioural analysis)	Data Protection Act 2018 (same as above) The Human Rights Act 1998 (same as above) The Equality Act 2010 (same as above)

15 SA Mathieson, 'How MI5 and MI6 Gather your Personal Data for Surveillance', (17 June 2016), available at: https://www.computerweekly.com/news/450298621/How-MI5-and-MI6-gather-your-personal-data-for-surveillance.

16 Liberty Investigates, 'UK Police Working with Controversial Tech Giant Palantir on Real-Time Surveillance Network', (16 June 2026), available at: https://libertyinvestigates.org.uk/articles/uk-police-working-with-controversial-tech-giant-palantir-on-real-time-surveillance-network/.

17 Dell Cameron, Wired, 'ICE Wants to Build Out a 24/7 Social Media Surveillance Team', (3 October 2025), available at: https://www.wired.com/story/ice-social-media-surveillance-24-7-contract/.

18 Security Service MI5, 'Analysing Intelligence'(accessed on 14 July 2026) available at: https://www.mi5.gov.uk/how-we-work/analysing-intelligence.

19 Department for Science, Innovation and Technology and the Rt Hon Peter Kyle MP, 'Press Release: AI to Help Police Catch Criminal Before They Strike', (15 August 2025), available at: https://www.gov.uk/government/news/ai-to-help-police-catch-criminals-before-they-strike.

20 Joseph Cox, 404, 'Elite': The Palantir App ICE Uses to Find Neighbourhoods to Raid', (15 January 2026), available at: https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid/.

21 Liberty Investigates, 'UK Police Working with Controversial Tech Giant Palantir on Real-Time Surveillance Network', (16 June 2026), available at: https://libertyinvestigates.org.uk/articles/uk-police-working-with-controversial-tech-giant-palantir-on-real-time-surveillance-network/.

1: Data collection

Large volumes of data. including personal data and special category data, are collected from a wide range of sources.

Privileged data received from other countries

Hacked data

Internet of things data

Open-source intelligence

Bulk data held by a third party

Bulk personal data (BPD)

Targeted communications data

CCTV/ Surveillance

Bulk communications data (metadata)

Social media intelligence

Electronic data protected by encryption

Intercepted Communications

2: Making the data useable

Raw data is cleaned, standardised, labelled and transformed into a useable format for AI models.

3: Using the data

The standardised data can be fed into AI models for a number of purposes, including:

ASSESSMENT

- Identity Verification
- Individual Risk Assessment
- Sentiment Analysis
- Predictive mapping
- Profiling (behavioural analysis)

TRAINING

Data may be used to teach AI models to make accurate predictions or find connections and patterns in data.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).