Owning the Code, Losing Control: How UK National Security Law Regulates AI and Intellectual Property

By Faizul Azman
3PB Barristers

This article analyses how the UK's export-control, patent secrecy and investment-screening regimes apply to artificial intelligence (AI) models and datasets that generate dual-use or defence-relevant outputs. It argues that legality turns on both capability and potential end-use: an AI system may require a licence because of its technical performance or because the exporter knows or suspects that its outputs could support weapons of mass destruction (WMD) programmes. Ownership of intellectual property (IP) therefore no longer guarantees freedom to use, license or transfer AI models. The article aims to show how public law controls intersect traditional IP rights and explains why, under the broad statutory definitions of "technology" and "software", AI models themselves can constitute controlled technology only where they meet a listed control specification or convey information necessary for the development, production or use of controlled items.

Introduction

AI and IP are converging in ways that test the limits of national security law. Organisations increasingly use their own IP – proprietary data, technical drawings, research and design documents – to train bespoke AI systems. These models can analyse, design and optimise with a sophistication once reserved for classified research programmes.

What begins as a tool for sustainable energy materials or manufacturing efficiency can, sometimes inadvertently, generate outputs relevant to weapons development or other defence applications. A dataset created from innocuous engineering drawings might be repurposed to improve missile components, or an algorithm designed for heat-resistant alloys might produce materials suitable for military propulsion.

AI models are themselves composed of IP assets. Their software code and architecture are protected by copyright, datasets may attract database rights or trade secret protection, and certain training methods or outputs may be patentable. An AI system is not merely a technological artefact but a bundle of IP rights. When such a system acquires defence or dual-use potential, those private rights fall within the reach of public law through export-control and national security regulation.

The UK's legal framework – comprising export controls, patent secrecy directions and the National Security and Investment Act 2021 (NSIA) – was designed to manage precisely these sensitivities. Yet, those regimes were drafted for a world of physical goods and human inventors, not for self-learning systems capable of synthesising knowledge autonomously. While those regimes have existed for decades, their application to intangible assets such as algorithms, datasets and model weights remains an evolving area, interpreted case by case by regulators such as the Export Control Joint Unit and Investment Security Unit.

As AI models increasingly sit between civilian innovation and strategic capability, a new question emerges: ***when does the capability or intended use of an AI system bring it within the scope of national security regulation?***

This article addresses that question, explaining how UK law bases control on both the *technical characteristics* of a system and the *exporter's knowledge or suspicion* of potential WMD use. It also sets out how these controls interact with IP rights and why AI models fall within the legal definition of *"technology"* and *"software"*.

Intellectual Property: From Protection to Restriction

At its core, IP law governs the creation, ownership and commercial exploitation of intangible assets – including AI models and their component parts such as software, datasets and algorithms – granting exclusive rights that enable creators to control and profit from their work.

The system assumes that innovation flourishes when ideas circulate under a framework of enforceable rights. Patents are granted in exchange for disclosure; copyright supports dissemination through licensing; trade secret protection facilitates collaboration under confidentiality. In every case, the policy objective is to incentivise innovation through managed disclosure.

National security law operates on a contrasting premise. Where IP law promotes publication, licensing and commercialisation, security regulation imposes secrecy and containment. Once a dataset, algorithm or invention acquires potential military or dual-use significance, ***public***

law overtakes private right. The owner may retain title, but their freedom to use, license or sell that IP may be curtailed by export-controls, secrecy or investment screening powers.

This marks a significant evolution in the innovation economy. IP, while still the legal reward for creativity, has become a regulatory hinge; a mechanism through which the state can slow, restrict or condition the disclosure and transfer of technologies that carry national security implications. Secrecy directions and investment screening do not remove ownership of IP but can temporarily suspend or condition its commercial use until clearance is granted.

AI as "Technology" and "Software" under Export Control Law

The Export Control Order 2008 (ECO 2008) defines *"technology"* as *"specific information necessary for the development, production or use of goods or software"*. While this definition is broad, an AI model will only fall within scope where it contains or conveys technical information required to develop, produce or use a controlled item. Whether trained model weights constitute 'specific information' remains debated, though regulators treat them as embodying technical knowledge when use for controlled applications.

Under this definition, an AI model's source code and training algorithms are *"software"* and *"technology"*; the weights, parameters or architecture of a trained model contain specific information necessary to use or reproduce its function and therefore constitute *"technology"*. Training datasets and documentation providing information for *"development"* or *"production"* also fall within the same scope.

In short, AI models are considered technology – digital artefacts containing the knowledge required to perform a controlled function. Transferring them electronically (whether by email, API, cloud, remote access) can amount to an export of controlled technology under the ECO 2008. The Export Control Joint Unit (ECJU) treats AI code, models and training data as potentially subject to licence where they embody controlled know-how.

The UK Legal Framework: Capability and End-Use Controls

The Export Control Act 2002 (ECA 2002)

The ECA 2002 provides the statutory foundation for the UK's export-control regime. Under section 1 of the ECA 2002, the Secretary of State may make orders controlling the export of goods, software and technology of any description, including by reference to their use or potential use, and may require a licence where necessary for reasons of national security or international obligations.

The ECA 2002 enables regulations to operate in two complementary ways"

- **Capability based controls**, which regulate items because of what they are or what they can do; and
- **End-use controls**, which regulate items of how they may be used or where the exporter knows or suspects that they could be used for prohibited purposes such as WMD programmes.

The Export Control Order 2008 and End-Use Controls

The ECO 2008 consolidated all prior export-control rules under one instrument, replacing earlier orders and expanding UK controls on the trade and transit of sensitive military and dual-use goods. The ECO 2008 applies to England, Wales and Scotland, while Regulation (EU) 2021/821 continues to apply directly in Northern Ireland under the Windsor Framework. The Order governs capability, end-use, transit and trade controls for military and dual-use goods; *see DBT's Guide to UK Strategic Export Controls*.

Capability-based control

Schedule 2 of the ECO 2008, as maintained by the UK Strategic Export Controls List, identifies goods, software and technology controlled because of their listed technical capability or performance threshold, irrespective of the exporter's knowledge or intent. Not all AI models will meet these thresholds, but if a model or dataset performs, or enables others to perform, a listed controlled function – such as missile guidance, propulsion, advanced cryptography or materials simulation (e.g., software "specially designed or modified for the development or production of rockets or UAV's" under Military List ML22.a) – it may require an export licence before transfer.

End-use control – WMD in the UK' wider scope in Northern Ireland

In England, Wales and Scotland, Article 6 of the ECO 2008 introduces end-use control limited to WMD purposes. A licence is required where an exporter knows, has been informed, or has reason to believe that otherwise unlisted goods, software or technology may be intended, in whole or in part, for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification, or dissemination of chemical, biological or nuclear weapons; or the development, production, maintenance or storage of missiles capable of delivering such weapons. This applies exclusively to WMD-related end-uses; there is no general military end-use catch all in England, Wales and Scotland. Conventional military

applications of unlisted technology are instead covered by the UK Military List (capability-based control) and destination-based embargoes in Article 4 and Schedule 3 of the ECO 2008.

In Northern Ireland, the broader EU Dual-Use Regulation (EU 2021/821) continues to apply directly under the Windsor Framework. Its Article 4 retains a wider 'catch-all', extending beyond WMD uses to certain military end-uses in embargoed destinations and, in some cases, human rights related concerns. This divergence is confirmed in the DBT guidance, *Export controls: dual-use items, software and technology, goods for torture and radioactive sources* (2025).

Example of Capability versus End-Use

A UK software company develops two AI models:

***Model A** autonomously generates designs for high temperature composite materials. The model's performance parameters meet those described in the UK Strategic Export Control List. It is controlled by capability – a licence is mandatory for an export.*

***Model B** is designed purely for civil aerospace and is not listed. However, during negotiations the company learns that a potential licensee manufactures missile components for nuclear capable systems. Even though the software itself is benign, the company's knowledge of potential end-use triggers the WMD end-use control under Article 6 of the ECO 2008, and a licence must be obtained before transfer.*

If however, the intended use were for missiles (albeit it can be argued that all missiles could be used to deploy WMDs), the Article 6 control would not apply; the transaction would only be caught if the software were specifically listed or the destination was embargoed.

Patent Secrecy

Section 22 of the Patents Act 1977 empowers the UK Intellectual Property Office (UKIPO) to issue secrecy directions where an invention is *"prejudicial to national security"*. Publication and foreign filing are prohibited until the direction is lifted.

While this mechanism functions effectively for military inventions, it does not yet extend to AI models, datasets or copyright works – leaving a gap between traditional patent control and modern, machine-generated outputs. Secrecy directions suspend publication and restrict use but do not extinguish ownership; enforceability resumes once clearance is granted.

Example: a company patents a heat-resistant alloy produced by its AI design model. When it seeks to license the patent overseas, the Export Control Joint Unit (ECJU) intervenes: the alloy could be used in missile propulsion. The patent remains valid, but disclosure of its specification without a licence would breach export law. Here, IP protection collides directly with national security control.

National Security and Investment Act 2021

The NSIA empowers the Secretary of State for Business and Trade to review, block or unwind acquisitions of *"qualifying entities or assets"* that may threaten national security. It establishes a standalone screening regime, separate from the export-control licensing, but frequently overlapping in practice when technology or AI assets are involved.

The definition of *"assets"* includes intellectual property rights, software, databases, algorithms, source code and trade secrets. This means that licensing or transferring rights in an AI model, dataset, or related IP can itself be treated as an acquisition of control subject to government review.

The National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulation 2021 (SI 2021/1264) identify 17 sectors requiring mandatory notification for certain corporate acquisitions, including artificial intelligence, advanced materials, computer hardware, defence and data infrastructure. While those regulations apply to acquisitions of qualifying entities, the Secretary of State also has broad call-in powers to review acquisitions of assets, whether notification was mandatory. Intervention may occur, for example, where a transaction could give foreign parties access to sensitive AI technology or datasets.

In 2022 the Government prohibited a proposed IP-licensing arrangement between the University of Manchester and a Chinese company, finding that the imaging technology could have military applications[1]. This first prohibition of a purely IP transaction confirmed that even intangible assets such as AI models, datasets or code can trigger state intervention.

The NSIA complements the export-control regime by regulating who owns or controls sensitive technology, rather than how it is transferred abroad. A company therefore may need both an export licence to share an AI model with a foreign party; and NSIA clearance if the transaction gives the foreign party control over the IP or model.

---

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092802/aquisition-scamp5-scamp7-know-how-final-order-notice-20220720.pdf

For practitioners, the implication is clear: any cross-border licensing or collaboration involving AI models or datasets should be assessed not only for export-licence requirements but also for potential notification or call-in under the NSIA, even where there is no change in corporate ownership.

When Civilian AI Becomes Controlled Technology

AI is collapsing the old boundary between civilian innovation and defence capability. AI models developed for commercial or academic use can generate results equally applicable to weapons, propulsion or surveillance systems. UK law therefore assesses both what the technology can do and what the exporter knows about its potential use.

For AI developers, IP ownership confers control over the model, its architecture and outputs; export-control and national security regimes then determine whether that control can lawfully be exercised across borders. In practice, most AI models will not currently trigger export licensing, but the framework allows ECJU intervention where outputs relate to listed or WMD applications.

Using Proprietary IP to Build AI Datasets

Many organisations now build AI datasets using their own proprietary IP – designs, experimental data and technical documents. Autonomy over inputs does not remove risk. If those inputs, or the resulting dataset, could assist in developing weapons, sensors or propulsion systems, they may fall under dual-use export controls.

Illustration: A renewable-energy company aggregates decades of research on high-temperature materials to create a dataset for AI based optimisation. The model performs well but also generates designs capable of withstanding combustion pressures used in rocket engines. The ECJU advises that the dataset and model cannot be shared with non-UK partners without a licence. The company still owns the IP but cannot lawfully commercialise it abroad.

AI Built from Open-Source or Public Data

Developers may use AI models trained on vast quantities of open-source data or publicly available information – scientific papers, patent databases, technical manuals and engineering datasets. The assumption is that because the underlying material is already in the public domain, the resulting model or outputs cannot raise export control concerns. That assumption is incorrect.

Under the ECO 2008, the focus is not on where the data originated but on *what the technology can do*. If an AI system processes open-source data to generate new designs, formulas or materials that could be used in weapons, propulsion or surveillance systems, those outputs can constitute controlled technology. Public availability of the inputs does not exempt the results from the regulation. Information already in the public domain or arising from fundamental research is generally excluded from control; however, where AI synthesises such data into new, non-public technical outputs relevant to controlled applications, licensing may still be required.

Illustration: A research consortium trains a large-language AI model on millions of publicly available academic papers and patent specifications relating to materials science. The purpose is to discover new heat-resistant alloys for space exploration and clean-energy turbines. The model succeeds – but also identifies a composite structure capable of maintaining stability at temperatures exceeding those of conventional rocket exhausts. When the consortium seeks to licence the AI platform to an overseas aerospace manufacturer, the ECJU intervenes. Although every data source was open and lawful, the *capability* of the resulting model to design military grade materials brings it within the scope of dual-use controls. A government licence is required before there can be any transfer abroad.

In this case, both the consortium and any downstream licensee may be responsible for ensuring compliance, illustrating that open-source research environments are not exempt from export-control obligations.

This example highlights a fundamental feature of export law: knowledge created by aggregation and inference can itself become controlled, even if each underlying data point was freely available. The act of synthesising open information through AI can produce results equivalent to classified research.

For organisations and practitioners, the compliance question therefore extends beyond data provenance. They must ask not only *"where did the data come from?"* but also *"what can this model now do?"*. The answer determines whether a system trained on open information is a harmless research tool or a licensable, restricted technology.

Universities, Employees and Research Institutions

Universities and research institutions are increasingly at the centre of this tension. Academic work that appears purely scientific may, in application, produce data or models relevant to defence technology. The University of Manchester case demonstrates this point: the

Government's prohibition of an imaging-technology licence under the NSIA was directed not at a defence contractor but an academic institution.

Other UK universities have likely faced similar scrutiny where AI projects funded for medical or environmental purposes generated outputs that could, with minor adaptation, enhance surveillance or targeting systems. Research collaborations involving foreign partners – particularly where overseas funding or data access is involved – are now subject to heightened due-diligence expectations. Institutions should maintain export-control policies and staff training, incorporating ECJU guidance.

Illustration: a postgraduate researcher develops an AI model for analysing fluid dynamics in offshore turbines. Without the researcher realising, the same algorithm can simulate air flow around missile fuselages. When the student takes employment overseas and proposes to continue development using the university code, the institution must consider export-control implications. What began as academic research becomes a licensable, or restricted, transfer of controlled technology.

Employees within private companies can create similar exposure. An engineer who repurposes a proprietary dataset for an AI side-project may inadvertently create a model where outputs fall within export-control parameters. The employer retains ownership of the IP but may bear compliance liability if that model is transferred abroad.

For both universities and employers, the lesson is clear: research governance and IP management policies must integrate export-control and national security review at the project design stage, not as an afterthought.

Commercial and Export Barriers

AI Systems and datasets with dual-use potential face three overlapping legal barriers. These frameworks overlap but serve different purposes: export control governs movement of technology, patent secrecy governs disclosure, and the NSIA governs ownership and control:

1. **Export control licensing** – required for any transfer "by any means" of controlled data, software or models;

2. **Patent secrecy directions** – which can suspend publication or licensing where an invention is security sensitive; and

3. **NSIA screening** – allowing government to prohibit or unwind transactions involving sensitive IP or AI assets.

Each barrier limits not ownership, but freedom to operate. A company may have valid IP rights yet be prevented from disclosing, licensing or selling its technology to particular partners or jurisdictions.

Practical example: a start-up develops an AI model for predicting stress fractures in lightweight materials. Its business plan is to license the model globally. During due diligence, an overseas investor is found to be state linked. The NSIA requires notification, and the ECJU indicates that export of the model weights may need a licence. Funding and launch are delayed while the regulatory position is clarified.

This is the new commercial reality: **licensing and regulatory clearance are now as important as ownership and originality.**

Failure to comply with export-control requirements is a criminal offence under Part 6 of the ECO 2008, punishable by imprisonment or unlimited fines. Civil penalties may also be imposed under the Export Control (Civil Penalties) Order 2019, and licences may be suspended or revoked under Article 32 of the ECO 2008. The regime is not purely strict liability; exporters are expected to demonstrate reasonable due diligence.

What Practitioners and Organisations Should Consider

Before embarking on costly AI or data-driven projects, organisations and advisers should:

1. **Assess the technology early** – mapping potential applications and identifying any defence adjacent outputs; and screen against the UK Strategic Export Control List and ECJU guidance.

2. **Classify and document** – maintain clear records of datasets, model purposes and risk assessments; and keep contemporaneous evidence of legal advice or regulator engagement to demonstrate due diligence if questioned.

3. **Structure agreements for compliance** – include end-use restrictions, export control warranties and audit rights; and impose territorial limits and sub-licensing conditions.

4. **Engage with regulators proactively** – seek guidance from the ECJU or the Investment Security Unit at an early stage; and consider voluntary NSIA notification for high-risk sectors.

5. **Budget for compliance** – factor export licensing timelines and legal costs into project planning; and consider that non-compliance may result in criminal liability, reputational damage and lost investment.

6. **Review cross-border collaborations regularly** – retaining or upgrading models may alter export-control status over time.

Policy Outlook

UK policy is moving towards closer alignment between AI governance and export-control. Commitments made at the AI Safety Summit and the UK's participation in G7, and OECD frameworks suggest that future regulation will focus on the diffusion of high-capability models and the export of training data. Practitioners should expect closer cooperation between technology regulators and the ECJU in the coming years. Actual alignment will depend on consultation outcomes and may evolve gradually.

Conclusion

AI has redefined how knowledge is created and applied, but it has not displaced the legal boundaries that govern its use. Enforcement remains proportionate and case-specific; not all AI activity falls within government control. Whether an AI system is trained on private, synthetic or open-source material, its lawful transfer depends on what it can do and what the exporter knows about potential WMD application.

If either threshold is met – capability or WMD end-use – export-control, secrecy and investment screening regimes may restrict or prohibit its transfer abroad. For developers, universities and investors, the key consideration is not merely IP protection but regulatory viability. Open science and national security law now coexist uneasily in the same digital space. Early engagement with the ECJU or the Investment Security Unit, and careful contractual and governance planning, are essential to avoid costly barriers to commercialisation.

For practitioners, the challenge is interdisciplinary: combining expertise in IP, technology and national security law to ensure that innovation remains both lawful and secure. In many cases, the AI model itself is an IP asset, its code, data and architecture protected by copyright, database right or confidentiality – yet those same rights are now circumscribed by public law constraints. Ultimately, while ownership remains fundamental, the decisive questions are capability, potential end-use and compliance – factors that determine whether innovation can safely cross borders.

This document is not intended to constitute and should not be used as a substitute for legal advice on any specific matter. No liability for the accuracy of the content of this document, or the consequences of relying on it, is assumed by the author. If you seek further information, please contact the 3PB clerking team on David.Fielder@3pb.co.uk

22 October 2025

Faizul Azman

Barrister
3PB Barristers

020 7583 8055
faizul.azman@3pb.co.uk

3pb.co.uk