

THE KNOWLEDGE

WWW.CORKERBINNING.COM

AUTUMN EDITION

From Salisbury to State Threats: The Transformation of UK National Security Law

Anna Rothwell

Beyond Ballistics: 3D Printed Firearms and the New Evidential Battleground

Gemma Motion

CPS to Prioritise Asset Recovery – a New Approach or Playing Catch-up?

Nick Barnard

JXM v SFO - Collateral Use of Investigatory Material Between Authorities

Joseph Hume

CORKERBINNING ^{CB}

09
2026

CONTENTS

4	From Salisbury to State Threats: The Transformation of UK National Security Law Anna Rothwell
14	Beyond Ballistics: 3D Printed Firearms and the New Evidential Battleground Gemma Motion
20	CPS to Prioritise Asset Recovery – a New Approach or Playing Catch-up? Nick Barnard
26	Patchwork Offending - Fraudulent Trading After R v Beckett Rebecca Hughes
32	JXM v SFO - Collateral Use of Investigatory Material Between Authorities Joseph Hume
40	Wright v Medway MC – Lessons in Transparency, Accountability and the Proper Exercise of Public Powers Lily Beweley-West
48	The Authority of a Postscript Edward Grange

WELCOME



Nick Barnard
Partner and Editor

Welcome to the Autumn 2026 edition of The Knowledge

After a foray into the world of sport for our summer edition, we return with a fresh batch of articles on a range of international and domestic criminal law issues:

- Anna Rothwell starts off with a review of the National Security Act 2023, and the shifting landscape of laws intended to counter state threats.
- Gemma Motion examines the new phenomenon of 3D printed firearms, and how their manufacture shifts the evidential focus from ballistics to digital forensics.
- I take a look at the two new Strategies published by the Crown Prosecution Service, and their focus on proceeds of crime and asset recovery.
- Rebecca Hughes, Joe Hume and Lily Beweley-West each analyse recent significant judgments on the boundaries of fraudulent trading, collateral use of evidence between investigations and the 'incidental' prosecutorial powers of state agencies.
- Finally, Edward Grange steps back and considers the evolution of judicial postscripts and how they shape our understanding and practice.

We hope you enjoy. If you missed our special digital-only Summer of Sport edition, or want to catch up on back-issues, you can find them all at corkerbinning.com/the-knowledge.

From Salisbury to State Threats: The Transformation of UK National Security Law

Anna Rothwell
Of Counsel

The attempted assassination of Sergei and Yulia Skripal in Salisbury in March 2018 by officers from Russia's GRU Volunteer Corps (a unit of the Russian military responsible for special or unconventional operations), triggered what has become a radical overhaul of the law in England & Wales relating to national security and counter-espionage.

The changes began with the introduction of the stop and search powers in Schedule 3 of the Counter-Terrorism and Border Security Act 2019 ("CTBSA 2019"), and progressed considerably with the introduction of the National Security Act 2023 ("NSA 2023"), the most significant national security legislation for almost a century, the core aim of which was to overhaul the outdated system of counter-espionage laws and counter modern threats from state actors. Both Acts are modelled on existing terrorism legislation, giving counter-terrorism police much greater investigatory powers and creating new offences that transform otherwise lawful or petty criminal activity into serious criminal offences attracting substantial prison sentences. According to the Independent Reviewer of State Threats, Jonathan Hall KC, in his latest annual report, with these Acts the UK has "tooled up" by granting major new powers to the authorities, updating old espionage laws,

and creating genuinely novel criminal offences such as 'foreign interference', 'sabotage', and 'assisting a Foreign Intelligence Service' ("FIS").¹

As noted by Mr Hall KC, given that such powers and offences extend well into the zone of political activity, journalism, protest and day-to-day human activity, they must be tested against misuse and overreach, however useful. This is particularly important given the lengthy deterrent sentences handed down so far to those convicted of offences under the NSA 2023.

Despite the NSA 2023 having been described as "extremely comprehensive" in evidence to a Parliamentary Committee as recently as October 2025,² this summer the National Security (States Threats) Act 2026 ("NSSTA 2026") has been rushed through Parliament in under a month, with only limited public and Parliamentary scrutiny. Within days of this Act receiving Royal Assent, on 17 July 2026 Parliament approved an order made by the Home Secretary "designating" (a new power similar to terrorist proscription) the group responsible for the Salisbury attacks – the GRU Volunteer Corps – which triggered the CTBSA 2019 changes, along with the Islamic Revolutionary Guard Corps ("IRGC") and the Islamic Movement of Companions of the Right ("IMCR"). It is now a crime to express support for these groups.³ The NSSTA 2026 has also facilitated the prosecution of those who assist or accept a material benefit such as payment from these groups, whether the individual acted intentionally or with wilful blindness.⁴

What are "state threats"?

State threats are defined by MI5 (the UK's domestic security service) as "overt or covert actions by foreign governments which fall short of direct armed conflict with the UK but go beyond peaceful diplomacy and expected statecraft to harm or threaten the safety or interests of the UK or our allies".⁵

They include not only what might be termed classic

"As noted by Mr Hall KC, given that such powers and offences extend well into the zone of political activity, journalism, protest and day-to-day human activity, they must be tested against misuse and overreach, however useful."

¹ See https://assets.publishing.service.gov.uk/media/69411a3eadb5707d9f33d7e8/E03512978_-_Un-Act_The_National_Security_Act_in_2024_Accessible.pdf

² See the evidence of Lord Sumption to the Joint Committee on the National Security Strategy, as referenced in their report on Espionage cases and the Official Secrets Acts, published on 3 December 2025, <https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/1414/report.html#heading-12>

³ Under section 2 of the NSSTA 2026, which inserts a new section 17A (support for a designated body) into the NSA 2023.

⁴ Under section 2 of the NSSTA 2026, which inserts new sections 17B (assisting a designated body) and 17C (obtaining material benefits from a designated body) into the NSA 2023.

⁵ MI5 website, <https://www.mi5.gov.uk/what-we-do/countering-state-threats> (last accessed 21.7.26).

espionage (i.e. the theft of sensitive information), or threats of physical violence, intimidation or assassinations, but also more modern-day concerns involving cyber-attacks, disinformation, and the theft of commercial or industrial information/targeting of academic research by states to support their own economy or technological and military capabilities.

In a speech on 16 October 2025, Sir Ken McCallum, Director General of MI5 described state threats as being of an equal or even greater magnitude than the threat from terrorism, with a 35% increase in the number of individuals being investigated for involvement in such activity in the past year. MI5 believes that at least 20 foreign intelligence services are still actively operating against UK interests.⁶ Recent arrests and prosecutions have involved nationals from countries as varied as the UK, Bulgaria, Hong Kong, Romania and Iran, who have been convicted of or alleged to have been acting on behalf of the Russian, Chinese and Iranian states and/or intelligence services.

Schedule 3 of the Counter-Terrorism and Border Security Act 2019

Jonathan Hall KC describes state threats as having been first “brought out of the shadows” by the terminology used in Schedule 3 of the CTBSA 2019, which is directed against “hostile activity”.⁷

Modelled on Schedule 7 of the Terrorism Act 2000 (“TACT 2000”), Schedule 3 gives the police powers to “examine” individuals at airports, seaports and the Northern Ireland border to determine whether the individual appears to be a person who is, or has been, “engaged in hostile activity”.⁸

An act is defined as hostile if it:

- i) threatens national security;
- ii) threatens the economic well-being of the United Kingdom in a way relevant to the interests of national security; or

iii) is an act of serious crime.⁹

Importantly, this power can be exercised by the examining officer whether or not that officer has grounds for suspecting that a person is or has been engaged in hostile activity.¹⁰ It is also immaterial:

- i) whether the person is aware that the activity in which they are or have been engaged is hostile activity; or
- ii) whether a State for or on behalf of which, or in the interests of which, a hostile act is carried out has instigated, sanctioned, or is otherwise aware of, the carrying out of the act.¹¹

Schedule 3 gives examining officers the power to stop, question, search and detain a person at a UK port for up to six hours. Individuals can be compelled to answer the examining officer’s questions (there is no right to silence) and hand over all PIN codes and passwords to their phones and laptops and any documents in their possession of a kind specified. Failure to comply may constitute a criminal offence.¹²

Importantly, Schedule 3 also allows examining officers to retain, copy, use and destroy devices found during a search. These powers are subject to the oversight of the Investigatory Powers Commissioner (“the Commissioner”) and it is strongly recommended that anyone stopped who has their devices seized and copied makes representations to the Commissioner. However, the powers given to the police by Schedule 3 are so broad that, following an amendment in the NSA 2023, not only can confidential business records be retained and reviewed but the Commissioner can authorise the retention and use by the police of confidential journalistic material, legally privileged material and medical records, provided it is used only so far as necessary and proportionate for a relevant purpose (i.e. in the interests of national security, the economic well-being of the UK where relevant to the interests of national security, to prevent or

"In a speech on 16 October 2025, Sir Ken McCallum, Director General of MI5 described state threats as being of an equal or even greater magnitude than the threat from terrorism"

⁶ <https://www.mi5.gov.uk/faq>

⁷ Ibid paragraph 1.1

⁸ CTBSA 2019, Schedule 3, Paragraph 1(1)

⁹ Ibid, paragraph 1(6)

¹⁰ Ibid, paragraph 1(4)

¹¹ Ibid, paragraph 1(7)

¹² Ibid, paragraph 23

"Unlike stops carried out under Schedule 7 of TACT 2000, statistics on Schedule 3 examinations are not currently published...However, anecdotally use of the powers appears to be increasing, particularly in relation to individuals connected to Russia or sensitive industries in China."

detect serious crime or to prevent death or serious injury) and is held securely. Parliament justified these powers – which exceed those under Schedule 7 TACT 2000 – by reference to the use of professional cover by foreign intelligence officers and their agents including journalists and lawyers.¹³

Unlike stops carried out under Schedule 7 of TACT 2000, statistics on Schedule 3 examinations are not currently published. Jonathan Hall KC reports that the numbers are lower than that under Schedule 7.¹⁴ However, anecdotally use of the powers appears to be increasing, particularly in relation to individuals connected to Russia or sensitive industries in China. One recent high-profile example involved Stephen Yaxley-Lennon (more commonly known as Tommy Robinson) who was reportedly recently stopped and examined under Schedule 3 after travelling to Russia.¹⁵ Mr Yaxley-Lennon has previously successfully challenged a charge of wilfully obstructing a search under Schedule 7 of TACT 2000 when he refused to hand the PIN number to his phone over to police;¹⁶ it remains to be seen if he challenges the retention of his data under Schedule 3.

The National Security Act 2023

Before the implementation of the NSA 2023, the Law Commission concluded in September 2020 that the three Official Secrets Acts (dating back to 1911, 1920, and 1939) were outdated and no longer fit for purpose. For instance, under those historic Acts, it was not an offence to be a covert agent of a foreign power, whilst espionage offences were “very wide but rarely prosecuted” as a result of archaic and obscure drafting and complex supporting case law. The Commission recommended replacing the term “enemy” with “foreign power” in any future statute. (That such outdated legislation was inadequate was vividly illustrated during the recent controversy surrounding the collapse of the high-profile espionage prosecution of Christopher Cash and Christopher Berry under the Official Secrets Act 1911.)¹⁷

¹³ Hansard (HL) Vol 793 Col 1888 (14.11.18), Minister of State.

¹⁴ https://assets.publishing.service.gov.uk/media/69411a3eadb5707d9f33d7e8/E03512978_-_Un-Act_The_National_Security_Act_in_2024_Accessible.pdf

¹⁵ <https://www.theguardian.com/uk-news/2026/jun/14/police-stop-tommy-robinson-way-back-london-from-russia>

¹⁶ <https://www.judiciary.uk/wp-content/uploads/2025/11/R-v-Stephen-Lennon.pdf>

¹⁷ For further detail see the UK Parliament Joint Committee on the National Security Strategy report into “Espionage Cases and the Official Secrets Act” published on 3 December 2025 at <https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/1414/report.html#heading-7>

"The NSA 2023 is aimed not just at deliberate state threat actors but also those who 'reasonably ought to have known' that they were involved in activity on behalf of a foreign power or FIS, especially those with knowledge (academics or those working in government), skills (ex-military acting as security operatives) or lack of inhibition (ordinary criminals)."

As a direct result of the Law Commission's findings, the NSA 2023 came into force on 20 December 2023. The NSA 2023 modernised the Official Secrets Acts' 'espionage' regime (repealing the 1911, 1920, and 1939 Acts) and created new offences, including:

- espionage offences: i) section 1 obtaining or disclosing protected information; ii) section 2 obtaining or disclosing trade secrets; and iii) section 3 assisting a foreign intelligence service ("FIS"). The section 1 and 2 offences (but not the section 3 offence) require the prosecution to establish that the conduct was carried out on behalf of a foreign power (as outlined in section 33).
- offences relating to foreign interference: i) a section 13 general offence and ii) section 16 election interference. Again, the foreign power condition applies to both offences. The section 13 offence is structured in a complicated fashion and, as well as requiring that the conduct has one of the multiple interference effects listed in section 14(1), it requires that one of three conditions listed in section 15 is met; i) the conduct in question must otherwise be an offence; ii) involve coercion of any kind; or iii) involve the making of a misrepresentation.
- offence of sabotage: found in section 12, this includes both damage to property and damage caused by cyber-attacks.
- offences relating to prohibited places: i) section 4 offence of entering a prohibited place for a purpose prejudicial to the UK and ii) section 5 unauthorised entry to a prohibited place, including via electronic or remote means.
- a preparatory conduct offence: under section 18, it is an offence for an individual to intend

to commit an offence under sections 1, 2, 4 or 12 NSA 2023. For example, three Iranian nationals were recently charged with section 18 offences (as well as section 3), namely surveillance, reconnaissance and open-source research, intending to commit acts/that acts would be committed by others, namely serious violence against a person in the UK.¹⁸

The Act also introduces a new Foreign Influence Registration Scheme ("FIRS") and enables the imposition of prevention and investigation measures ("PIM") similar to TPIMs used in terrorism legislation.

To date, the majority of arrests under the NSA 2023 have been for section 3, assisting a foreign intelligence service, or section 18, preparatory conduct. Notably, the section 3 offence does not require the 'foreign power' condition to be satisfied, unlike the majority of other NSA 2023 offences. In order to establish the 'foreign power' condition, it must be proven that a person's conduct, or course of conduct of which it forms part, was carried out 'for or on behalf of a foreign power' and the person either knew or 'having regard to other matters known to them ought reasonably to have known' that this was the case. The effect of this condition (as a gateway to the related NSA 2023 offences) is that conduct that is otherwise lawful, constitutes only a more minor offence, or is wrongful only as a matter of private law, is an offence if carried out on behalf of, or with the intention of benefiting, a foreign power i.e. some other (part of a) state or its government. For example, surveillance routinely undertaken by security companies of those accused of insurance or other fraud, could become unlawful if carried out on behalf of a foreign police or intelligence service. In a recent trial that we acted in, the jury convicted the defendants of a section 3 offence, but was unable to convict in relation to the arguably more legally and factually complicated section 13 foreign interference offence that had been charged,

¹⁸ <https://www.cps.gov.uk/cps/news/three-men-charged-national-security-act-offences>

"Rather than relying on the existing statutory framework, Parliament has rushed through new legislation with limited scrutiny. Although the House of Lords did incorporate defences for humanitarian activity and a "reasonable excuse" defence for obtaining, accepting, or agreeing to accept information from a designated body, concerns remain regarding the necessity and proportionality of the new measures."

which required both the prosecution to establish that prohibited conduct had occurred, and the foreign power condition.

The NSA 2023 is aimed not just at deliberate state threat actors but also those who "reasonably ought to have known" that they were involved in activity on behalf of a foreign power or FIS, especially those with knowledge (academics or those working in government), skills (ex-military acting as security operatives) or lack of inhibition (ordinary criminals). This adds an element of objectivity, potentially resulting in individuals being prosecuted for what they 'should' have known and risking unjust outcomes, particularly given the serious nature of the offences and lengthy deterrent penalties. Jonathan Hall KC has cautioned that this could drag in the naïve or ill-informed, noting that it may be necessary to consider omitting the word "reasonably" or to provide a statutory defence that the defendant did not in fact suspect the matter of which he is accused.¹⁹

The National Security (State Threats) Act 2026

The new NSSTA 2026 was introduced following Mr Hall KC's review of whether additional powers modelled on counter-terrorism legislation were necessary to combat state-based security threats. There had been calls for certain state-backed groups to be proscribed under terrorism legislation, including the IGRC. Mr Hall KC, however, concluded that it was not appropriate to proscribe a state entity, as this would stretch the definition of terrorism beyond its intended meaning.²⁰

A key recommendation in his report – which has now been implemented in the NSSTA 2026 – was to develop a state threats proscription-style power, in order to do more to warn the public (in particular those criminals, proxy groups, misfits and private investigators who might be tempted to assist) about the risk posed by the most dangerous organisations, and to allow the government to communicate decisive stigma at an international level.²¹

It remains unclear why the existing offences under the NSA 2023 could not be used to prosecute the individuals concerned. In particular, some of those recently arrested appear likely to have been acting on behalf of organisations that were subsequently designated. Rather than relying on the existing statutory framework, Parliament has rushed through new legislation with limited scrutiny. Although the House of Lords did incorporate defences for humanitarian activity and a "reasonable excuse" defence for obtaining, accepting, or agreeing to accept information from a designated body, concerns remain regarding the necessity and proportionality of the new measures.

As Mr Hall KC acknowledged in his report, the designation regime risks harming civil liberties, including freedom of association and expression; distorting the ordinary criminal law through the use of special measures; increasing suspicion towards certain nationalities; and causing adverse effects for innocent family members. While Mr Hall KC concluded that these concerns must be balanced against the threat posed by aggressive FIS to individual rights and national security, it is nevertheless difficult to see why the existing NSA 2023 offences are inadequate. Indeed, many of the activities identified in the Explanatory Notes to the National Security and State Threats Act (NSSTA) would already appear to constitute criminal offences under the NSA 2023.²²

Consequently, the new legislation appears less concerned with addressing a genuine gap in the law than with signalling a strong public message and further facilitating prosecutions under already broadly drafted offences. It remains to be seen if this has a chilling effect on journalists or results in an increased risk of unjust prosecutions of unwitting or naïve individuals.

"The new legislation appears less concerned with addressing a genuine gap in the law than with signalling a strong public message and further facilitating prosecutions under already broadly drafted offences."

²² The examples given in the Explanatory Note include:

- a foreign intelligence service obtaining protected information and inspecting sensitive defence or intelligence sites in the UK (a "prohibited place") (see new sections 33(3)(a)(i) and (iv) of the NSA, as inserted by the NSSTA),
- a mercenary group carrying out acts of serious violence on behalf of a foreign power (see sections 33(3)(b) and (4)(a) of the NSA, as inserted by the NSSTA), or
- a network preparing to carry out sabotage or threatening to commit acts that create a serious risk to the health and safety of the public with the intention of benefiting a foreign power in doing so (see sections 33(3)(a)(v) – (b) and (4)(c) of the NSA, as inserted by the NSSTA).

¹⁹ Ibid, paragraph 2.57

²⁰ <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2025/05/19.5.25-State-Threat-and-Terrorism-report-1.pdf>

²¹ Ibid, paragraph 5.7

Beyond Ballistics: 3D Printed Firearms and the New Evidential Battleground

Gemma Motion
Associate

A decade ago, firearms prosecutions typically began and ended with an exhibit: a gun, recovered, examined and traced back to its origin. The emergence of 3D printed guns has changed all that.¹

Creating a 3D printed firearm usually involves downloading a digital blueprint, processing it through slicing software, printing plastic components, and assembling them with metal parts. As a result, it can now be the case that the most significant item recovered by investigators is not the weapon itself but a laptop or digital blueprint. The firearm may be merely the end product of what looks more like a cybercrime investigation than a conventional firearms prosecution. The shift matters because it will reshape where the real battles in firearms prosecutions are fought: not over ballistics, but disclosure.

Steel to software

The principal statute governing firearms in England & Wales is the Firearms Act 1968, which lays out a comprehensive regime for their control, regulation and prohibition. The Act mandates a certification system for those allowed firearms.² Certain other weapons are specifically prohibited (such as those that are automatic) and accordingly there is a general prohibition making it an offence to possess, manufacture, sell or transfer these items without written authority from the Secretary of State.³

Despite its age, the Act has proved more adaptable than might be expected. A complete and functioning 3D printed firearm can fall within the section 57

definition just as a traditional firearm produced by a licensed manufacturer could. That said, Parliament has been alive to the fact certain changes are necessary. The (partially in force) Border Security, Asylum and Immigration Act 2025 introduces new offences of possessing, making, adapting or supplying “relevant articles” for use in connection with serious crime.⁴ Amongst other things, this includes a 3D printer firearms template.⁵ This is a reasoned move as the issue is no longer merely theoretical and recent years have demonstrated an increase in dangerous 3D weapons printing and resulting prosecutions.⁶

Taking but one example, the case of Robert Adamski saw recovery of a 3D printer in Adamski’s east London flat mid-production of a rifle component alongside a second, further advanced printed firearm. Adamski was convicted of two counts of possessing a prohibited firearm, together with terrorism offences, and sentenced to fifteen years’ imprisonment.⁷ What is instructive is how the case was built: a saved digital manufacturing guide, software recovered from the printer’s SD card, and messages from a Telegram account created and operated by Adamski. These constituted the evidential backbone linking him to manufacture. A firearms expert was still required to confirm the weapon’s capability but it is clear that much of the case centred on digital attribution.

A shift in the evidential centre of gravity

A conventional firearm begins life as a recognisable weapon, albeit in some cases (for example, replica

¹ The first UK conviction in the UK for manufacturing a 3D printed gun was the case of Tendai Muswere (jailed in September 2019 as a result of events occurring in 2017) <https://www.bbc.co.uk/news/uk-england-london-49761290>

² Sections 26 – 31, Firearms Act 1968

³ Section 5, Firearms Act 1968

⁴ Section 52, Border Security, Asylum and Immigration Act 2025

⁵ Section 53, Border Security, Asylum and Immigration Act 2025

⁶ By way of example: <https://www.bbc.co.uk/news/uk-england-leeds-65612574> and <https://www.bbc.co.uk/news/articles/c2lk87qkzg4o>

⁷ <https://www.cps.gov.uk/cps/news/man-jailed-printing-3d-gun-parts-london-flat>

"Establishing the prosecution case may depend as much on reconstructing a digital chronology as on any forensic firearms examination."

or deactivated firearms) one that might later be modified or converted. A printed firearm begins life somewhat in reverse as a Computer Aided Design ("CAD") file on a computer and polymer components printed separately over time – harmless in isolation but lethal when finally combined with metal parts to produce a fully functioning weapon. That timeline changes what the prosecution must prove.

Searches increasingly recover CAD files, encrypted messaging records, browser histories and cryptocurrency transactions alongside or instead of completed weapons. Establishing the prosecution case may depend as much on reconstructing a digital chronology as on any forensic firearms examination. That reconstruction raises fresh questions: who downloaded the file? Who operated the printer? Did failed attempts reflect genuine experimentation or a step towards manufacture? Those sorts of questions cannot be answered purely by examining the firearm itself. Defence practitioners will be familiar with matters of digital attribution from cases involving other offences, but perhaps not yet in the sphere of firearms offences.⁸

Disclosure

Because of this shift in the evidential centre of gravity, the Criminal Procedure and Investigations Act 1996 ("CPIA") will assume a new significance when compared against conventional firearms cases. Section 3 of the CPIA imposes the well-known continuing duty on the prosecution to disclose material that might reasonably be considered capable of undermining the case for the prosecution against the accused or assisting the case for the accused. In a case simply built around a recovered weapon, identifying such disclosable material is likely to be much more straightforward than in one involving terabytes of digital material.

In cases concerning 3D printed guns, investigators will seize laptops, mobiles and external drives and

recover from them multiple versions of CAD files, deleted documents and fragments of encrypted communications. It is probable that much of that material will not be relied upon by the prosecution but will still fall to be disclosed under the CPIA regime. As with all cases, individually unremarkable items within that unused material may fit together in a manner decisively helpful to the defence.

The Attorney General's Guidelines on Disclosure now place particular emphasis on proportionate digital strategies and early engagement between parties specifically because of cases like this, involving volumes of data that would have been unthinkable until recent years.⁹ That emphasis reflects a genuine tension: examining every byte of seized material may be neither necessary nor proportionate but a proportionate review must not shade an incomplete one. This is particularly the case where the central issue may turn on the interpretation of a chronology of downloads or print attempts. Quite obviously, a precise defence statement that identifies issues like authorship of a file, control of a printer or an innocent explanation for possession of CAD files is more likely to sharpen disclosure obligations and assist the defence than one focused on a bare denial.

Cross-border issues

There may be further complications as a consequence of manufacturing chains which can easily cross borders in a way that traditional firearms legislation was not designed to accommodate. A file could be designed abroad, stored on a foreign server, downloaded in England, then combined with components sourced from other countries.

In such cases, investigators may find that the evidence necessary to establish authorship, control or the chronology of design is held not by a UK entity but by a foreign platform operator or manufacturer. Obtaining that material may require formal mutual legal assistance ("MLA") in the form of a request under

⁸ By way of example, indecent images, computer misuse or drug trafficking

⁹ Attorney General's Guidelines on Disclosure 2024, Annex A (digital material)

"The emergence of 3D printed guns within the UK highlights more of a shift in the evidence than a gap in the law."

section 7 of the Crime (International Co-operation) Act 2003. Such requests allow for designated courts and prosecutors to issue them, particularly where measures like compelled production of data or search and seizure are needed. Alternatively, if the material sought is electronic evidence held by a service provider outside the UK, a different route may be available under the Crime (Overseas Production Order) Act 2019, which can allow a UK court to make an order directly enforceable against an overseas communications service provider without the need for a full MLA request.

These are just two examples of other pieces of legislation that may assume pronounced significance in a 3D firearms prosecution. Practically speaking, disclosure timelines in cases like these are more likely to be contingent on the cooperation of foreign authorities, the designation status of the requested country, and the speed with which letters of request are executed abroad.

Conclusion

The emergence of 3D printed guns within the UK highlights more of a shift in the evidence than a gap in the law. The existing statutory framework certainly has not been rendered obsolete despite the fact that its drafters could never have envisaged this modern development. Especially with subsequent amendments, the core offences remain capable of catching conduct in this new era. What has changed is the practical reality of investigation and disclosure. A truly modern firearms case may increasingly consist of metadata as opposed to a single recovered weapon and this is important for criminal practitioners to understand. Future legal developments in this area are unlikely to be decided principally by arguments over the Act itself, but rather on a case-by-case basis in disputes over what digital material was disclosed, what was left unexamined, and whether the chronology presented by the prosecution at trial can withstand the scrutiny of the forensic process that produced it.

CPS to Prioritise Asset Recovery – a New Approach or Playing Catch-up?

Nick Barnard
Partner

When an organisation publishes material of any depth or complexity, it is often worth reviewing the accompanying publicity to identify what message the organisation is seeking to deliver – and how that compares to the substantive content. In the case of the UK Crown Prosecution Service (“CPS”), two new strategies were published in June 2026 addressing its approach to Serious & Organised Crime (“the SEOC Strategy”) and international investigations and prosecutions (“the International Strategy”). Applying the above approach of comparing message with content, what is the CPS hoping the world at large will take away from them?

The two strategies cover a number of issues and initiatives. In the SEOC Strategy, the CPS sets out how it plans to combat the increasingly transnational and interconnected nature of organised crime, and its amplification by developing technology. Organised crime is also presented as a growing threat to national security, particularly through money-laundering, human trafficking and ‘scam centre’ fraud conducted on an industrial, international scale. The CPS plans to respond to these threats by increasing its own technological capability (inevitably, AI is mentioned) and strengthening collaboration with other UK and international agencies. In a similar vein, the International Strategy sets out how the CPS will improve its ‘capability and confidence’ and relationships with foreign prosecutors and other agencies to enable it to more effectively conduct cases

where the evidence, suspects or assets are overseas.

As is clear from the above, both strategies concern a raft of issues spanning the most serious and complex areas of criminal justice for which the CPS is responsible. Considering that breadth of scope, it is striking that the supporting press release (*‘Prosecutors to proactively target illegal assets to ensure crime does not pay under new CPS strategies’*) leans almost exclusively on asset recovery as the focus of efforts to fight organised crime. In particular, the CPS intends to:

- i) Consider asset recovery opportunities at an earlier stage in SEOC cases – which will presumably require increased cooperation with investigative agencies, and result in increased numbers of restraint orders.
- ii) ‘Modernise’ its civil recovery capability such that its Civil Recovery Unit can ‘operate more efficiently, consistently and at scale’.
- iii) Increase its international activity and cooperation, both in terms of seeking overseas assistance and providing assistance to foreign authorities seeking to recover assets in this jurisdiction.¹

Whilst an uptick in asset recovery does indeed feature in both Strategies, it is only one of several areas of focus within each. Given there have been no major developments in recent years in the legislation or powers available to target criminal property, why has the CPS chosen to major on this point? Before

¹ One wonders whether the CPS may have seen an advance copy of Jonathan Fisher KC’s report on Fraud in the Digital Age, published in July 2026, Recommendation 27 of which is ‘Use trade agreements and memorandums of understanding to promote international law enforcement cooperation on evidence gathering, asset recovery, and extradition in fraud/economic crime cases affecting UK residents’

addressing that question, it is worth considering the current landscape of criminal asset freezing and forfeiture in the UK.

Many of the powers available under the Proceeds of Crime Act 2002 ("POCA") – for example, obtaining restraint orders during investigations, or applying to freeze and forfeit cash and/or the contents of bank or crypto accounts – are available to a wide group of UK organisations. As well as the obvious law enforcement and regulatory agencies (for example, the National Crime Agency ("NCA"), Serious Fraud Office ("SFO"), Financial Conduct Authority ("FCA") and HM Revenue & Customs ("HMRC")), any state body acting through a suitably authorised Accredited Financial Investigator can seek such orders. This is the mechanism by which – for example – departments within local authorities can freeze and seize assets to combat trading standards, benefit fraud or planning breach offences. In its everyday work prosecuting acquisitive crime, the CPS will frequently obtain restraint orders at the point of charge (if not already in place from the investigation stage) and seek confiscation orders on conviction. Where property cannot be recovered directly from an offender for whatever reason, Civil Recovery Orders enable recovery on application to the High Court with no need for any related conviction.² However, all this activity is – or at least has been until now – ancillary to the CPS's core function of prosecuting offences.

By contrast, the NCA has a much clearer mandate to pursue asset recovery as a standalone activity. On the dissolution of the Asset Recovery Agency in 2008, its functions were folded into the predecessor Serious Organised Crime Agency, and now live on in the NCA's dedicated Civil Recovery and Tax team. As an investigative rather than prosecutorial agency, the NCA also has additional investigative powers under POCA. Most notably, although Unexplained Wealth Orders ("UWOs") are available to all of the HMRC, FCA,

SFO and CPS (via the Director of Public Prosecutions), the NCA has been the exponent since their creation by the Criminal Finances Act 2017, having made 22 of the 23 applications so far. As well as its own endeavours, the NCA is also responsible for the Proceeds of Crime Centre, which trains and monitors Accredited Financial Investigators to carry out POCA investigations and proceedings both within the NCA and other agencies.

So, bearing in mind that little has changed in the POCA landscape, and that the CPS is by no means the only agency with POCA powers and remit, why has it chosen this moment to announce a renewed focus on its asset recovery activities?

There is undoubtedly a political angle, with early and specific mention of targeting people smugglers who – although undoubtedly causing huge harm – occupy a disproportionate slice of the political and media agenda. It is also true to say that – as mentioned in both Strategies – there is an increasing impetus to address the types of criminality which go beyond considerations of criminal justice to matters of national security, including human trafficking, money laundering and industrialised international fraud.

There has also been growing recognition in recent years (as reflected in the significant changes made by the Criminal Finances Act 2017) that targeting assets alongside or even instead of prosecutions is a legitimate – and effective – means of combating serious, organised and international crime. The appeal of asset deprivation and recovery in such criminality is twofold. Firstly, the nature of the offending and offenders often make for poor prospects of successful prosecutions in the UK, particularly where suspects and evidence are situated overseas. Secondly, the exercise is both punitive – depriving the offenders of their ill-gotten gains – but also preventative – by cutting off the cash

"Bearing in mind that little has changed in the POCA landscape, and that the CPS is by no means the only agency with POCA powers and remit, why has it chosen this moment to announce a renewed focus on its asset recovery activities?"

² See for example, the current Civil Recovery Order proceedings resulting from the Lantian Gerui Fraud – in which the CPS has found itself in possession of Bitcoin worth several billion, concerning which the court must now decide between the competing interests of UK and Chinese authorities and individual victims.

flow, further offending is curtailed.

The explosion in economic sanctions activity since the Russian invasion of Ukraine provides a neat parallel for this evolving philosophy, as agencies worldwide have collaborated to target not individual persons and entities but their assets. Although there are always disputes as to whether a particular subject should or should not be designated, there seems little disagreement that targeting assets is a valid means of achieving the overall aim.

Even the SFO has shown an increasing enthusiasm for such activity, having trumpeted both its first UWO (the only instance not spearheaded by the NCA) and first Crypto-Wallet Freezing Order in the course of 2025. Its POCA update page, which has previously seen between three and four entries per year, had already hit six announcements by July 2026. For the SFO, the increased focus on asset recovery – despite it not being part of its core remit – may in part be financial, as agencies involved in successful POCA recovery processes generally receive 50% of the bounty under the Asset Recovery Incentivisation Scheme. This is in stark contrast to the huge sums obtained by the SFO (in excess of £1.7bn) under Deferred Prosecution Agreements since 2015, all of which was surrendered to the Treasury. The move may also be existential: every SFO failure – of which there have been all too many in recent years – triggers fresh discussion on whether it should be folded into the NCA or another larger agency. Perhaps by flexing its POCA muscles, the SFO is seeking to prove its worth as an independent enterprise.

Whilst the CPS is unlikely to face any similar threat, its senior management will inevitably have been considering the agency's future. Rather than simply pledge to do the same things (but somehow better and more efficiently), it makes good sense to explore new avenues to prevent and disrupt serious,

organised and international crime, particularly those avenues where success can both be empirically measured and swell the coffers. There are principled objections in response – in particular, what disincentive is there against carrying out serious organised crime in the UK from the safety of another jurisdiction, if the only downside risk is the loss of (some of) your bottom line? However, the CPS would inevitably fall back on realpolitik – whilst it is not ruling out the prospect of pursuing prosecutions in the UK (with the assistance of extradition and other mutual legal assistance channels where necessary), it would be remiss not to deploy every available tool in parallel, particularly where those tools have been proven effective elsewhere.

In considering how the Strategies might play out in practice, it should be recognised that any focus on asset recovery can only be a reprioritisation rather than a revolution. There does not appear to be any new money or resources for the CPS, nor is there any new legislation to make the task easier. Whilst the CPS is undoubtedly on trend in focussing on asset recovery, that is not the same as delivering results without compromising its work elsewhere. The NCA does at least justify some of its focus on asset recovery through its investigatory remit, as well as its historic functions. By contrast, the CPS is – at its core – a prosecutor and must take care to avoid sacrificing important work for easy wins.

“The CPS is – at its core – a prosecutor and must take care to avoid sacrificing important work for easy wins.”

Patchwork Offending - Fraudulent Trading After R v Beckett

Rebecca Hughes
Senior Associate

The Court of Appeal in *R v Beckett*¹ is the latest authority to examine the scope of fraudulent trading under section 993 of the Companies Act 2006. The decision follows neatly from *R v Hunter*² and earlier authorities but cements a broader trend in the prosecution and sentencing of fraudulent trading, with potentially wider implications for both civil and corporate criminal liability.

In dismissing Mr Beckett's appeal, the Court revisited the meaning of "fraudulent purpose" and took an expansive view of the circumstances that may engage section 993. The Court confirmed that prosecutors are not required to prove any specific acts of misconduct. Rather, a fraudulent purpose may be proved from a cumulative 'patchwork' of acts and omissions.

The Appeal

Mr Beckett appealed his conviction and sentence on two counts of fraudulent trading contrary to section 993 of the Companies Act 2006:

"If any business of a company is carried on with intent to defraud creditors of the company or creditors of any other person, or for any fraudulent purpose, every person who is knowingly a party to the carrying on of the business in that manner commits an offence."

Mr Beckett was the sole director of NIG Installs Limited and The Insulate Group, companies that sold insulation and roof coating products.

The prosecution alleged that both companies were fundamentally dishonest, systematically deploying unfair commercial practices to obtain custom and targeting the elderly and vulnerable. These practices included misleading consumers about the condition of their existing insulation, misrepresenting product performance and employing high-pressure sales techniques to dissuade customers from exercising their statutory cooling-off rights. The prosecution's case was that Mr Beckett either knew these practices were being used, or they formed "*part of the sales culture which he put in place*".³ On that basis, it argued that the offence of fraudulent trading was complete; it was not necessary to prove deception or an intention to deceive on Mr Beckett's part.

The defence accused the prosecution of cherry-picking evidence that did not reflect the general activities of the business. Mr Beckett claimed to believe the statements contained in the sales scripts and characterised some of the false claims as "*normal commercial puffery*".⁴ To the extent that problematic practices occurred, he denied knowledge of them.

The appeal raised five grounds, all concerning the trial judge's directions or answers to the jury. The central issue, pervading the first and third ground, was the judge's directions on the meaning of "fraudulent purpose". The judge directed that "*fraudulent purpose implies an intention to behave in a way which goes beyond the bounds of what ordinary decent people engaged in business would regard as honest*";⁵ but that the offence did not require proof of deception, an intention to deceive or even completed sales.

The meaning of "fraudulent purpose"

The Court of Appeal endorsed the trial judge's directions as consistent with the approach in *R v Hunter*.⁶ In *Hunter*, the Court of Appeal reviewed the authorities on section 993 and clarified that (i) dishonesty was an essential ingredient of fraud; (ii) fraud and deception are not synonymous; and (iii)

¹ *R v Beckett* [2026] EWCA Crim 462

² *R v Hunter and Another* [2021] EWCA Crim 1785

³ *R v Beckett* [2026] EWCA Crim 462

⁴ *Ibid.*, at [21]

⁵ *Ibid.*, at [23]

⁶ *R v Hunter and Another* [2021] EWCA Crim 1785

"The Court in Beckett definitively rejected the submission that the prosecution must prove some form of specific misconduct, confirming that this is not an ingredient of the offence."

a fraudulent purpose may be proven before anyone has been defrauded or suffered loss.⁷

In addition to applying these principles, however, the Court in Beckett definitively rejected the submission that the prosecution must prove some form of specific misconduct, confirming that this is not an ingredient of the offence. It held that:

"A fraudulent purpose may be proved from a patchwork of acts and omissions, or planed [sic.] acts and omissions, including acts which could be described as misconduct, which, taken together, prove the fraudulent purpose."⁸

It follows that a fraudulent purpose may arise from the cumulative effect of conduct which, viewed individually, may be characterised as commercially aggressive, negligent or 'sharp' trading practice, but taken together, crosses the threshold of criminality.

In endorsing this approach, Beckett shifts the evidential focus away from a particular fraudulent transaction towards the overall character of the business. In cautioning against attempts to define "fraudulent purpose", the Court confirmed the extent of the scope of behaviour that may amount to, or contribute to, the offence, and the evidential basis upon which prosecutors may seek to establish it.

Criminal defence practitioners may recognise parallels with the offence of controlling or coercive behaviour. The Crown Prosecution Service ("CPS") guidance for that offence emphasises that individual incidents, viewed in isolation, may seem innocent – or at least not criminal – but the cumulative impact can become so when considered within the wider context of the relationship.

The analogy is not exact, but both offences occupy an unusual position in criminal law; often relied upon by prosecutors where the relevant conduct does not fit comfortably within other statutory offences. In the case of Beckett, aggressive tactics and false

claims notwithstanding, the victims received the goods that they paid for. It bears little resemblance to the typical boiler room fraud (see, for example, the highly publicised case of *R v Ryan*⁹). Faced with the decision in Beckett, prosecutors may feel emboldened to pursue fraudulent trading where, historically, the common law offence of conspiracy to defraud would be charged: an especially attractive prospect in light of the Court's comments in Beckett on sentencing.

The future of sentencing

The Court's endorsement of the prosecution's approach in Beckett reflects a willingness to use the full force of the criminal law to deter sustained commercial misconduct. The Court made no critical comment on the prosecution's decision not to charge offences under the Consumer Protection from Unfair Trading Regulations 2008,¹⁰ acknowledging that those offences were time-barred and do not require proof of dishonesty. The dismissal of Mr Beckett's appeal against his sentence likewise confirms judicial appetite to ensure that fraudulent trading attracts appropriately deterrent sentences.

Beckett adds to a growing body of case law applying the sentencing principles set out in *R v Mackey*,¹¹ but distinguishing that case on its facts to justify lengthier prison sentences and director disqualification orders. Mackey recognised that the offence of fraudulent trading covers a wide spectrum of conduct, and subsequent courts have demonstrated a willingness to impose deterrent sentences where the trading is characterised as "deliberate"¹², "sustained"¹³ or targeted at vulnerable victims.¹⁴ In Beckett, the Court described the fraudulent enterprise as "cold-blooded, deliberate and cruel" in justifying Mr Beckett's sentence of six and a half years' imprisonment (over four times the sentence imposed in Mackey).¹⁵

The Court ultimately adopted the trial judge's basis for sentence as limited to the scope of the fraudulent purpose evidenced at trial. This is consistent with the

"The Court's endorsement of the prosecution's approach in Beckett reflects a willingness to use the full force of the criminal law to deter sustained commercial misconduct."

⁷ Ibid., at [118 – 120]

⁸ *R v Beckett* [2026] EWCA Crim 462, at [40]

⁹ *Ryan v R* [2022] EWCA Crim 1347; City of London Police: Duo sentenced to a total of 19 years in jail after large scale investment fraud

¹⁰ Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277)

¹¹ *R v Mackey* [2012] EWCA Crim 2205, at [16(5)]

¹² *R v Ali* [2019] EWCA Crim 1263, at [37]

¹³ *R v Rattu* [2020] EWCA Crim 757, at [13]

¹⁴ *R v Beckett* [2026] EWCA Crim 462, at [109]

¹⁵ Ibid., at [109]

"The Court's approach in Beckett highlights the distinction between the civil and criminal provisions, and may result in more cases being referred for criminal investigation and prosecution where insufficient or no loss is established, or else the culpability of individual defendants demands a deterrent response."

Court of Appeal's approach in *R v Ali*¹⁶ and *R v Rattu*.¹⁷ However, the Court's obiter remarks lend support to a broader sentencing approach, permitting inference of a fraudulent purpose beyond that directly evidenced. This fits with the Court's expansive interpretation of the meaning of "fraudulent purpose" but, in practical terms, risks deterrent custodial terms based on conduct that the jury did not necessarily find to be proved and may not have been invited to consider. Unlike the offence of controlling or coercive behaviour, fraudulent trading does not benefit from detailed Sentencing Council guidelines. Given the potential breadth of conduct that may now fall within scope, this appears an obvious area for development.

Wider implications

The Court's treatment of "fraudulent purpose" may also turn out to be significant in civil and corporate crime contexts.

First, the language of section 993 mirrors that of section 213 of the Insolvency Act 1986, insofar as liability can bite where there is proof of a fraudulent purpose. Section 213 is a civil provision that empowers the court, during the winding up of a company, to require persons who were "knowingly parties" to fraudulent trading to make contributions to the company's assets for the benefit of creditors. The purpose of Section 213 is therefore compensatory, with the court's focus on making good any loss to creditors, rather than punishing the underlying dishonest conduct.

It remains to be seen whether *Beckett*'s expansive interpretation of "fraudulent purpose" will find favour in a civil context. Given the materially different purpose of section 213, the direct impact may be limited. Nonetheless, the Court's approach in *Beckett* highlights the distinction between the civil and criminal provisions, and may result in more cases being referred for criminal investigation and prosecution where insufficient or no loss is established, or else the culpability of individual

defendants demands a deterrent response.

Second, the potential reach of *Beckett* must be considered in light of the Economic Crime and Corporate Transparency Act 2023 ("ECCTA"). Fraudulent trading is one of the offences listed in Schedule 13, to which the section 199 corporate offence of failure to prevent fraud applies. Following *Beckett*, "large organisations"¹⁸ would be wise to review their fraud prevention procedures, reflecting the increased risk that an employee or agent may be found with the requisite intent to have carried on part of their business for a fraudulent purpose.

The Home Office guidance makes clear that the failure to prevent offence does not require a completed fraud or financial gain. However, *Beckett* arguably expands the range of conduct capable of evidencing fraudulent trading. If prosecutors are entitled to rely upon a cumulative assessment of commercial practices, rather than proving specific acts of misconduct, organisations may need to review how they identify and protect against such practices, many of which may be embedded within the organisation's culture or regarded as commonplace in an industry. Particularly in sectors such as real estate, which is infamous for sharp trading practices and exposed to financial crime risks,¹⁹ risk assessments and internal training may need updating.

Conclusion

Viewed narrowly, *Beckett* is a clearer articulation of existing principles. However, by confirming that a fraudulent purpose may be established from a cumulative 'patchwork' of acts and omissions, the Court has shifted the evidential focus onto a wider range of conduct, bringing into scope 'sharp' trading practices previously considered a civil or consumer protection issue. In this way, the Court's expansive approach in *Beckett* may well encourage more prosecutions for fraudulent trading and invite deterrent sentences without proof of loss, as well as potentially widening the scope of related civil and corporate liability.

"Following Beckett, 'large organisations' would be wise to review their fraud prevention procedures, reflecting the increased risk that an employee or agent may be found with the requisite intent to have carried on part of their business for a fraudulent purpose."

¹⁶ *R v Ali* [2019] EWCA Crim 1263

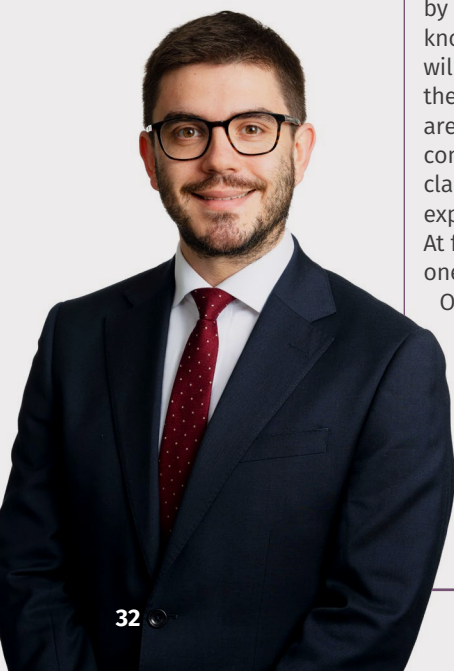
¹⁷ *R v Rattu* [2020] EWCA Crim 757

¹⁸ Section 201, Economic Crime and Corporate Transparency Act 2023

¹⁹ See for example, National Risk Assessment of Money Laundering and Terrorist Financing 2025; OFSI's "Property and Related Services: Threat Assessment" (April 2025); and the SFO's recent investigation into allegations of bribery and fraud by previous management at Home REIT, a social housing company (January 2026).

JXM v SFO – Collateral Use of Investigatory Material Between Authorities

Joseph Hume
Senior Associate



As any white-collar criminal solicitor will tell you, complex economic crime rarely falls neatly within the bailiwick of a single authority. Such investigations are typically capable of attracting a multitude of crosshairs, all focussed on different aspects of the offending behaviour.

To provide an illustrative example, assume one is advising a senior employee of a UK company who has allegedly secured a lucrative overseas contract by paying millions of pounds to a local consultant, knowing that a substantial proportion of the payment will be passed to government officials to influence the award of the contract. Naturally, those payments are disguised in the company's books as legitimate consultancy fees. The company's accountants then claim the consultancy payments as deductible business expenses, thereby reducing its corporation tax liability. At first blush, the substantive offending is clearly one of bribery and corruption and the Serious Fraud Office ("SFO") and its overseas counterparts might be expected to take an interest. However, the ordinary business processes that flow from such activities may also result in allegations of money-laundering and even tax evasion.

A scenario such as the one described above is rarely easy for the authorities to detect. Indeed, it may only come to the attention of a single authority in a seemingly benign way – often upon

discovery of some peripheral or otherwise innocuous irregularity. Let's say in the above example, HM Revenue & Customs ("HMRC") has noticed that errors have been made in the claims for tax deductions and is seeking an explanation. At that point, HMRC has a small strand in its grasp, without knowing the full extent of what has gone on. The danger here for the employee and their advisers is that HMRC has the potential to unravel the entire plot, if not itself then by alerting other authorities to the new threads that have become exposed.

The Statutory Framework

Given the increasing prevalence of such scenarios, the boundaries between criminal prosecutors, financial regulators and tax authorities – both domestically and overseas – have become increasingly porous. Information provided to one authority can find its way into the hands of another, often for an entirely different investigative purpose. However, information sharing is not a free-for-all and there is a statutory framework to govern it. To be alert to the risks, it is important to understand how information sharing between authorities operates.

Information sharing between HMRC and the UK authorities

The law on information sharing between HMRC and other authorities is principally governed by the Commissioners for Revenue and Customs Act 2005 ("CRCA 2005") and the Anti-Terrorism, Crime and Security Act 2001 ("ATCSA 2001"). The basic approach of these two statutes is to restrict the sharing of confidential information but prescribe a set of permitted exceptions.

CRCA 2005

The general confidentiality obligation is created by section 18(1) of CRCA 2005, which imposes a general prohibition on HMRC officials disclosing information held in connection with their functions. This prohibition

"The boundaries between criminal prosecutors, financial regulators and tax authorities – both domestically and overseas – have become increasingly porous. Information provided to one authority can find its way into the hands of another, often for an entirely different investigative purpose."

"The claimant sought to challenge, inter alia, the SFO's decision to open an investigation, its applications for search warrants (which partly relied upon information that JXM had provided to HMRC as part of a civil tax investigation, which HMRC had subsequently provided to the SFO), and Southwark Crown Court's decision to grant those warrants."

is broadly expressed and pervasive, save for the exceptions explained in section 18(2) below.

CRCA 2005 section 18(2) provides specific exceptions where disclosure is permitted. These include:

1. if the disclosure is made for the purposes of a function of HMRC and does not contravene any restriction imposed by the Commissioners. Essentially this means that information can be disclosed internally within HMRC, or to other parties, but only if the disclosure is necessary for HMRC to carry out its statutory functions, such as the collection and management of taxes or the administration of tax credits;
2. if the disclosure is made in accordance with section 20 or 21 of the Act;
 - (a) section 20 is on public interest grounds;
 - (b) section 21 refers to disclosure to a prosecuting authority for the purpose of considering criminal proceedings;
3. if it is made for the purposes of civil proceedings relating to a matter in respect of which HMRC has functions;
4. if it is made for the purposes of a criminal investigation or criminal proceedings relating to a matter in respect of which HMRC has functions i.e. passing potentially incriminating material to HMRC's Fraud Investigation Service;
5. if it is made in pursuance of a court order;
6. if it is made to certain inspectorates for the purposes of inspection;
7. if it is made to the Director General of the Independent Office for Police Conduct for the exercise of relevant functions;
8. if it is made with the consent of each person to whom the information relates; and

9. for certain devolved tax and VAT purposes.

ATCSA 2001

Section 19 of ATCSA 2001 concerns the disclosure of information held by HMRC departments. It provides that obligations of secrecy do not prevent the disclosure of such information if the disclosure is made for the purposes of any criminal investigation or proceedings (whether in the UK or elsewhere), for the initiation or conclusion of such investigations or proceedings, or to determine whether they should be initiated or concluded. However, any disclosure must be proportionate to the objective sought to be achieved and can only be made by, or with the authority of, the Commissioners. Further disclosure is restricted and generally requires the consent of the Commissioners, except for certain specified purposes. Importantly, nothing in section 19 authorises disclosures prohibited by data protection legislation. Furthermore, it does not prejudice any other existing powers to disclose information

Section 18(1) CRCA 2005 may give the impression that a protective wall exists to prevent HMRC from sharing information both internally and externally. However, in truth, through the carve-outs in section 18(2) of the same Act and section 19 ATCSA 2001, it could be more properly described as a protective sieve. As such, defence lawyers and their clients should have careful regard for the statutory gateways that allow for information sharing between prosecutorial authorities¹, as neatly illustrated in the recent judgment in *JXM v The Serious Fraud Office and Southwark Crown Court*.

Information sharing in action

In February 2026,² the Administrative Court in *JXM v Director of the Serious Fraud Office and Southwark Crown Court*³ refused permission for judicial review of decisions taken by the SFO and Southwark Crown Court in connection with Operation Zesty: an investigation into alleged bribery and money-laundering by

¹ For example, the similar frameworks of statutory information-sharing powers for the SFO, NCA and FCA through the Criminal Justice Act 1987, the Crime and Courts Act 2013 and the Financial Services and Markets Act 2000 respectively.

² This judgment was handed down in February 2026 but only became public in June 2026.

³ <https://www.judiciary.uk/wp-content/uploads/2026/06/JXM-v-SFO-and-Southwark-Crown-Court.pdf>

"The decision is a timely reminder of why investigations require careful navigation and why baring one's soul (even in circumstances where a criminal investigation is not afoot) might not produce the cleansing experience that the authorities may promise."

individuals at the company Blu-3 concerning data centre construction contracts. The claimant sought to challenge, inter alia, the SFO's decision to open an investigation, its applications for search warrants (which partly relied upon information that JXM had provided to HMRC as part of a civil tax investigation, which HMRC had subsequently provided to the SFO), and Southwark Crown Court's decision to grant those warrants.

JXM made three submissions:

1. The SFO should not have opened its investigation, and continued to receive and rely on material from HMRC in circumstances where he had willingly cooperated in a civil tax investigation, without HMRC warning that it might later be used against him in a criminal investigation, thereby infringing the privilege against self-incrimination.
2. The SFO should not have been able to apply for search warrants against JXM because, although the material in its possession was sufficient to establish suspicion, the SFO should never have received the documents from HMRC upon which it based those suspicions.
3. As a direct result of ground two, Southwark Crown Court should not have granted the application for search warrants.

The court rejected JXM's arguments on all three fronts.

Firstly, it held that the statutory gateways in the CRCA 2005 and ATCSA 2001 expressly permitted HMRC to disclose information for criminal investigations, making the transfer of information to the SFO lawful. The fact that JXM handed over the information in pursuit of cooperation in a civil tax investigation does not prevent the flow of information via the statutory gateways.

The court further rejected the challenge to the search warrants. It found that the SFO had reasonable

"Extreme care should be afforded when providing information, whether voluntarily, in response to an information notice or through COP9. As experienced by JXM, the resulting consequences can stretch far beyond initial expectations."

grounds to suspect serious fraud and that, following *Haralambous v Crown Court at St Albans*,⁴ material capable of supporting a search warrant application need not be admissible at trial. Even if self-incrimination arguments were ultimately relevant at trial, they did not prevent the information secured lawfully from being relied upon to obtain a warrant. In the interest of completeness, JXM also tried to argue that there had been a material non-disclosure under this ground also. The Court dismissed this out of hand because it could not realistically have affected the judge's decision to issue the warrants.

Finally, JXM's third submission failed on the same basis as submission two above.

The decision is a timely reminder of why investigations require careful navigation and why baring one's soul (even in circumstances where a criminal investigation is not afoot) might not produce the cleansing experience that the authorities may promise.

Conclusion

All of the above is to say that white-collar practitioners are right to be concerned when it comes to collateral use of material. This rings particularly true for those advising individuals in tax investigations. Whilst the mechanics of an HMRC investigation can feel less threatening (given the immunities afforded by the Code of Practice 9 ("COP9") process, the often informal negotiations in face-to-face meetings and the potential for investigations to take a civil rather than criminal course), this is no reason to lower one's guard. Extreme care should be afforded when providing information, whether voluntarily, in response to an information notice or through COP9. As experienced by JXM, the resulting consequences can stretch far beyond initial expectations.

⁴ [2018] 2 W.L.R. 357, SC

THE KNOWLEDGE FULL COMMENT



THE CORKER BINNING PODCAST

Full Comment from The Knowledge

Takes a look through a legal lens at stories in the news, as well as items that might not make the headlines, but deserve to be discussed, explored and given full comment.

Listen to the *Full Comment* podcast on the Corker Binning website, Spotify or Apple Podcasts

Wright v Medway MC – Lessons in Transparency, Accountability and the Proper Exercise of Public Powers

Lily Beweley-West
Associate



Those familiar with regulatory prosecutions may consider themselves well-acquainted with the range of statutory offences that are usually the subject of such proceedings. However, the recent case of *R (on the application of Matthew Wright) v Medway Magistrates' Court*¹ illustrates why practitioners should be careful not to narrow their horizons to what is usual or obvious. In confirming the scope of the Environment Agency's prosecutorial powers, the Divisional Court took the opportunity to affirm important principles relating to the privacy of charged individuals, the rights of different organisations to bring prosecutions, and the duty of candour in judicial review proceedings. What started as a challenge to an environmental law prosecution has grown into a case with considerably wider significance.

In rejecting an application for permission for judicial review brought by Matthew Wright, the former CEO of Southern Water, the Divisional Court confirmed that the Environment Agency's prosecutorial powers are not limited to offences within the Environmental Act 1995 ("the Act"). The underlying prosecution concerned an allegation of conspiracy to defraud, arising from the manipulation of wastewater treatment works intended to circumvent the Environment Agency's quality monitoring regime. It is understood to be the first time an officer of

a water company has faced criminal proceedings for an environmental crime. Mr Wright sought to judicially review the issuance of the summons on the basis that the Environment Agency did not have the statutory power to prosecute this type of offence.

The Environment Agency's Prosecutorial Powers

The Environment Agency was established by the Act, and has a broad regulatory and enforcement remit spanning pollution control, water resources, waste management, conservation and environmental compliance. It applied for summons against Mr Wright and three other suspects (who did not participate in the judicial review proceedings), which was granted by Medway Magistrates' Court. The Environment Agency relied on section 37(1) of the Act, which provides that the Environment Agency:

(a) *may do anything which, in its opinion, was calculated to facilitate, or was conducive or incidental to, the carrying out of its functions;*

[...]

and the Agency may institute criminal proceedings in England and Wales.

Mr Wright's argument was that the Environment Agency is a statutory corporation which lacks the common law powers to bring a private prosecution or

"The recent case of *R (on the application of Matthew Wright) v Medway Magistrates' Court* illustrates why practitioners should be careful not to narrow their horizons to what is usual or obvious."

¹ *R (on the application of Matthew Wright) v Medway Magistrates' Court* [2026] EWHC 1842 (Admin)

the Crown Prerogative to do so. It was contended that the Environment Agency's prosecutorial powers were limited to those expressly or impliedly conferred by statute. Counsel for Mr Wright suggested that the 'hanging' phrase of, "**and** the Agency may institute criminal proceedings" (emphasis added) meant that it must be read in conjunction with section 37(1)(a), and was therefore confined to offences prescribed by environmental legislation. As such, non-environmental statutory offences, common law offences and inchoate offences such as conspiracy, attempt or accessory liability all fell outside of the Environment Agency's prosecutorial powers.

The Environment Agency took the reverse stance, that the phrase should be read disjunctively from the earlier subsection, and that it conferred a general power in relation to any criminal offence. It cited *R v Rollins*,² which dealt with the Financial Services Authority's ("FSA") prosecutorial powers. In the alternative, the Environment Agency contended that prosecuting the offence of conspiracy to defraud in this specific case was incidental to its functions, in accordance with section 37(1)(a).

The Divisional Court refused the application, favouring the alternative argument made by the Environment Agency. It was held that section 37 enables the Environment Agency to bring a prosecution for any type of offence where it is capable of being calculated to facilitate, or conducive or incidental to the carrying out of its functions, and where in the Environment Agency's opinion, the prosecution is so facilitative, conducive and incidental. It was further held that "functions" encompasses all of the Environment Agency's powers and duties.

Mr Wright's arguments were rejected for four reasons:

- (a) To limit the Environment Agency's prosecutorial powers to statutory offences under environmental legislation within its

area of responsibility and exclude inchoate forms is reading words into the statutory provision which are not there.

- (b) It would produce unreasonable and anomalous results. For example, it would prevent the Environment Agency from prosecuting criminal damage following deliberate pollution or sabotage of flood defences, gross negligence manslaughter in relation to management of the environment within its responsibilities, or blackmail following a ransom cyber-attack on its computer systems. Equally, whilst it could prosecute a single individual for a statutory environmental offence, such as dumping toxic waste in a river, it could not prosecute a group who conspired to do so if their plans were thwarted.
- (c) It is inconsistent and incoherent to suggest that the prosecutorial powers do not extend to conspiracies, financial crime, dishonesty and fraud, as the Act itself contains a fraud and dishonesty offence.³
- (d) The remaining arguments made by Mr Wright, relating to the history of the offence of conspiracy to defraud considered in *R v Hayes and Palombo*,⁴ the limited investigation powers in section 108; the proposition that a statutory body cannot have a power incidental to an incidental power; and the Regulatory Enforcement and Sanctions Act 2008, all fell down when unpicked.

The Divisional Court also rejected the primary argument put forward by the Environment Agency (i.e. that it wields a general power to prosecute any offence) as contrary to section 37's heading of "incidental general functions". It also distinguished *R v Rollins*, as in that case it was held that the FSA,

³ Section 110(3) prescribes an offence of falsely pretending to be an authorised person investigating environmental offences.

⁴ *R v Hayes and Palombo* [2025] UKSC 29

² *R v Rollins* [2010] UKSC 39

"It would be strange if Parliament had intended to create a new agency, with specific functions but general powers of prosecution. To go beyond the general principle that statutory bodies' powers are confined to those conferred by statute, expressly or impliedly, would require very clear words from Parliament."

as an incorporated company, had the same power as a private individual to prosecute, whereas the Environment Agency is a statutory body, with its powers to prosecute found in, and only in, section 37. Although critical of the coherence of Mr Wright's arguments, Lord Justice Popplewell was cautious not to cast the net too wide. He took the opportunity to highlight the establishment of the Crown Prosecution Service, some ten years before the Act, as the dedicated state body with power to prosecute any and all offences within its jurisdiction. Against that backdrop, it would be strange if Parliament had intended to create a new agency, with specific functions but general powers of prosecution. To go beyond the general principle that statutory bodies' powers are confined to those conferred by statute, expressly or impliedly, would require very clear words from Parliament.

The Principle of Open Justice

Mr Wright was granted anonymity in the proceedings, under the cypher CVB, pending the outcome of the judicial review application. As such, the Divisional Court's refusal of permission automatically set this aside. Lord Justice Popplewell made clear, though, that he would have refused anonymity regardless of the outcome and overturned the original anonymity order.

The Court considered four recent authorities on anonymity: *Khuja v Times Newspapers Ltd*;⁵ *R (Rai) v Winchester Crown Court*;⁶ *ZXC v Bloomberg LP*;⁷ and *R (Marandi) v Westminster Magistrates' Court*.⁸ Lord Justice Popplewell summarised the key principles:

- (a) The general rule at common law is that the administration of justice must be done in public; the public has a right to know what is going on in the courts and who is involved.
- (b) Within freedom of expression are two important public interests: journalistic freedom of expression, which applies

⁵ *Khuja v Times Newspapers Ltd* [2017] UKSC 49

⁶ *R (Rai) v Winchester Crown Court* [2021] EWCA Civ 604

⁷ *ZXC v Bloomberg LP* [2022] UKSC 5

⁸ *R (Marandi) v Westminster Magistrates' Court* [2023] EWHC 587 (Admin)

to all media reporting, and open justice to promote public confidence in the administration of justice.

- (c) Restrictions on open justice are only permitted where truly exceptional and strictly necessary.
- (d) This approach applies to criminal and civil proceedings.
- (e) Whether an individual has a reasonable expectation of privacy pursuant to Article 8 of the European Convention on Human Rights is subject to a two-stage test: firstly, whether Article 8 rights are engaged at all, and secondly, whether they are balanced with Article 10 rights.
- (f) Damage to reputation following publication is not enough for Article 8 to be engaged. The injury to reputation must be sufficiently serious, considering the extent to which the information is in the public domain, and the extent to which damage to reputation is a foreseeable consequence.
- (g) There can be no reasonable expectation of privacy if a person is charged with a criminal offence, in contrast to a person subject to a criminal investigation prior to charge.

The Divisional Court found that Mr Wright's evidence of reputational harm did not give a reasonable expectation of privacy, given that his reputation had already been impacted by Southern Water's 51 convictions and his high-profile role in a major public utility company. This is a clear affirmation of judicial reluctance to depart from open justice.

The Duty of Candour

The Divisional Court also issued a stark reminder of the importance of the duty of candour. The Administrative Court had considered Mr Wright's application for anonymity on an urgent basis

because it had not been told that the return date in the criminal proceedings had been adjourned by two weeks. The Environment Agency subsequently applied to discharge the anonymity order for Mr Wright's breach of the duty.

The Divisional Court agreed that this was a breach, and deemed it a serious one. It was held that judicial review claimants are under an important and continuing duty to fully disclose material facts to the court, and that *"it is the strongest in urgent cases when interim remedies are sought"*. Lord Justice Popplewell cast doubt over whether the Administrative Court would have made the order as a matter of urgency had the true position been known. Mr Wright argued that the application was still urgent in the context of the adjourned date, however this was rejected and deemed no excuse for his failure to notify.

The Environment Agency was also criticised for breaching its own duty of candour in failing to notify the Court promptly. The Environment Agency did include the fact of the adjournment in its written submissions; however, these were only filed the day before the urgent hearing was listed.

Despite the seriousness of Mr Wright's breach, the Divisional Court ultimately held that it would not have justified the setting aside of the anonymity order (if it were otherwise to remain in force).

Whilst rooted in environmental crime and regulation, the significance of *R (on the application of Matthew Wright) v Medway Magistrates' Court* extends beyond statutory interpretation. It illustrates the breadth of statutory prosecutorial powers that Parliament may confer upon specialist regulators, reaffirms the constitutional importance of open justice in criminal proceedings, and underscores the rigorous duty of candour expected of those seeking public law remedies.

"Whilst rooted in environmental crime and regulation, the significance of R (on the application of Matthew Wright) v Medway Magistrates' Court extends beyond statutory interpretation. It illustrates the breadth of statutory prosecutorial powers that Parliament may confer upon specialist regulators, reaffirms the constitutional importance of open justice in criminal proceedings, and underscores the rigorous duty of candour expected of those seeking public law remedies."

The Authority of a Postscript

Edward Grange
Partner

The common law has always been meticulous in distinguishing different sources of legal authority. It has, however, been less careful in distinguishing different sources of judicial authority.

The recent decision in *Tobosaru & Tofan v Romania*¹ illustrates why the distinction matters. Having dismissed the substantive appeals, Mr Justice Sweeting appended a postscript in which he observed that two authorities cited on behalf of the Crown Prosecution Service (“CPS”) did not exist. They had apparently been generated through the use of artificial intelligence and had not been identified through human verification. The CPS apologised unreservedly. The court accepted there had been no intention to mislead, acknowledged the steps taken to prevent a recurrence, and observed that artificial intelligence is likely to become an increasingly important – and potentially beneficial – feature of legal practice, provided that appropriate safeguards are observed.

The postscript was careful, measured and proportionate. It also attracted almost as much attention as the judgment itself. That is hardly surprising. Lawyers instinctively attach significance to judicial observations, and so they should. The question is whether we always do so for the right reason.

A judgment derives its authority from more than judicial office. It is the product of a disciplined process. The parties define the issues. Evidence is tested. Arguments are advanced and challenged. The court explains why one side succeeds and the other does not.

Authority flows from that process as much as from the identity of the decision maker.

A postscript serves a different purpose. It forms part of the judgment but is not ordinarily necessary to the determination of the issues before the court. Instead, it looks beyond the dispute. It may comment on professional standards, litigation conduct or wider issues affecting the administration of justice that have become apparent during the proceedings.

Judges occupy a unique position within the legal system. They see recurring problems that individual practitioners may experience only occasionally. Sometimes those problems deserve wider attention than the dispute itself.

Mr Justice Sweeting’s postscript illustrates the point. Had the non-existent authorities not been identified, the consequences in another case might have been serious. His observations were not directed towards criticism for its own sake. They were directed towards protecting the integrity of the justice system.

The question is how such observations should be read. Historically, English judges have shown considerable discipline in separating the determination of disputes from wider reflections on the law. Lord Bingham demonstrated that judges contribute to the law in different ways. His judgments decided cases. His Hamlyn Lectures and other extra judicial writing shaped the wider legal conversation. Their influence was no less profound because they were not precedent. Indeed, the distinction formed part of their authority.²

The modern postscript sits slightly outside the traditional architecture of the common law. It forms part of the judgment but is not ordinarily necessary to determine the issues before the court. Nor is it extra judicial writing. Its place within our understanding of judicial authority is less certain. That distinction is easily overlooked because both appear beneath the same heading: “Judgment”.

“Judges occupy a unique position within the legal system. They see recurring problems that individual practitioners may experience only occasionally. Sometimes those problems deserve wider attention than the dispute itself.”

¹ [2026] EWHC 1720 (Admin)

² Historically, English judges have tended to express wider reflections on the law through reasoned *obiter dicta*, lectures, essays, textbooks and where appropriate formal reviews or law reform reports. The use of a separate, labelled postscript as a vehicle for broader observations is a comparatively modern judicial practice.

"The postscript in *Tobosaru & Tofan* reminds us that judges sometimes speak to the profession as well as to the parties before them. It has also prompted an important discussion about the responsible use of artificial intelligence. "

For practitioners, however, it matters. Those of us who spend our professional lives analysing judgments know how quickly a single paragraph can influence the way a case is understood. Sometimes it influences the way the profession behaves. A carefully expressed observation is reproduced in case summaries, discussed at seminars and cited in skeleton arguments. Before long, practitioners begin speaking of what "the courts expect", notwithstanding that no court has actually determined the point as a matter of law.

That is not a criticism of judges. Nor is it a criticism of practitioners. Rather, it is a reflection of the authority that judicial office properly commands. Respect for the different and distinct elements of a judgment should not slip into conflation. The authority of judicial reasoning derives from the determination of legal rights after evidence and adversarial argument. The authority of a postscript derives from the experience, judgment and perspective of the judge who has chosen to identify a wider issue revealed by the proceedings. They derive their authority from different sources.

The postscript in *Tobosaru & Tofan* reminds us that judges sometimes speak to the profession as well as to the parties before them. It has also prompted an important discussion about the responsible use of artificial intelligence. That discussion will no doubt continue.

The common law has always depended upon careful thinking about authority. It should be no less careful in thinking about the authority of judges themselves. The distinction is easy to overlook. The common law has rarely been well served by overlooking such distinctions.

Postscript

Nothing in this postscript is necessary to the argument. That seemed an appropriate place to end.

"The common law has always depended upon careful thinking about authority. It should be no less careful in thinking about the authority of judges themselves. The distinction is easy to overlook. The common law has rarely been well served by overlooking such distinctions."

CORKERBINNING

CORKER BINNING
4TH FLOOR
1 ELY PLACE
LONDON EC1N 6RY
+44 (0)20 7353 6000 (24HR)
WWW.CORKERBINNING.COM

Please contact our Administrator, Lucy Leite, on ll@corkerbinning.com,
if you do not wish to receive further editions of The Knowledge