Is the United Kingdom striking the right balance between National Security and the Right to Privacy?

In *Klass v Germany (1978) 2 EHRR 214, [§49]*, the European Court of Human Rights (ECtHR) recognised that laws framed to defend democracy can, if left unchecked, erode the very liberties they exist to protect. The Court cautioned:

"States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."

It is a warning which resonates with particular force today, when the demands of national security confront human rights, enshrined in both domestic and European law. At the heart of this tension lies the interplay between the collective right to life and security, protected under *Article 2* of the European Convention on Human Rights (ECHR), and the individual's right to privacy under *Article 8*. *Article 2* imposes upon states a positive and absolute duty to protect life, permitting no derogation, even in times of emergency. In *Osman v United Kingdom (1998) 29 EHRR 245, [§115],* the Court affirmed that states must adopt "operational measures" to shield individuals from known threats. Yet Strasbourg jurisprudence has equally made clear that even the mere possibility of covert surveillance suffices to engage *Article 8*, regardless of whether the information gathered pertains to private or public matters (*Malone v United Kingdom (1985) 7 EHRR 14*). Thus, the former binds the state with an unyielding obligation, while the latter yields only to lawful, proportionate, and necessary interference in a democratic society.

What distinguishes the current security landscape, however, is the reemergence of existential threats. Russia's expanding nuclear posture and increasingly confrontational stance have revived serious concerns about the possibility of strategic conflict between major powers. This is not merely theoretical. The state's duty under *Article 2* to avert loss of life now extends to threats that could unfold on an unprecedented scale. In this light, the test of proportionality under *Article 8* cannot be assessed in a vacuum. It must reflect the severity, complexity, and asymmetry of contemporary risks, including those that do not manifest through conventional violence but through data breaches, cyber sabotage or intelligence blind spots.

This essay asserts that the United Kingdom has formed a sophisticated legal and institutional framework which, in principle, strikes a lawful and proportionate balance between national security and privacy rights. Nevertheless, this balance remains fragile, continuously tested by evolving threats and technological change. The question is not merely whether laws exist on paper, but whether they function effectively in practice, and whether they remain sufficiently robust to withstand the pressures of a changing world.

The Modern Security Context

The United Kingdom's conception of national security has profoundly changed in recent years, driven by the rise of complex threats from hostile state actors. For the first time since the Cold War, the *National Security Strategy (NSS)*[1] published in June 2025 explicitly recognises "state-level threats across the spectrum of conflict," including the possibility of conventional armed attack. This represents an evident broadening of focus beyond the traditional post-9/11 emphasis on terrorism. While terrorism remains a severe threat, the contemporary landscape includes clandestine operations, cyber espionage, disinformation campaigns, and covert economic influence. Modern threats are no longer confined to bombs and bullets, but increasingly manifest through technological intrusions and influence operations, requiring a recalibration of the state's defensive measures and the legal frameworks that support them.

Recent incidents demonstrate how state adversaries have expanded their operations in the UK. The 2018 Salisbury poisoning[2] revealed the lethal reach of Russian operatives acting under plausible deniability. Meanwhile, the People's Republic of China (PRC) has engaged in extensive cyber intrusions and influence operations. In 2022, MI5 issued a *Security Service Interference Alert* naming London-based solicitor Christine Lee as an agent engaged in "political interference" on behalf of the Chinese Communist Party; a claim upheld as lawful by the Investigatory Powers Tribunal[3]. This incident demonstrates the UK's more assertive stance in countering foreign interference within its democratic institutions.

These threats highlight how modern adversaries operate in the so-called "grey zone,"[4] where the boundaries between peace and conflict are indistinct. Cyber intrusions, disinformation, and covert data exfiltration, while less overt than terrorism, pose significant threats to national security and the integrity of democratic institutions. The internet and social media have given adversaries a host of opportunities for hostile interventions and it is within this shifting geopolitical environment that the UK's legal framework balancing national security measures and privacy must now be assessed.

[1] HM Government, *National Security Strategy 2025: Security for the British People in a Dangerous World* (Cm 7890, June 2025) https://www.gov.uk/government/publications/national-security-strategy-2025
[2] House of Commons Foreign Affairs Committee, *Moscow's Gold: Russian Corruption in the UK* (HC 932, 2017–19) para 15–22 https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/932/932.pdf
[3] *Christine Lee & Daniel Wilkes v Security Service* [2024] UKIPTrib 7, para xx. Available at: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/12/Lee-Wilkes-Investigatory-Powers-Tribunal-judgment-17-December-2024.pdf
[4] Council on Geostrategy, *Foreign Interference in Democratic Societies: A Strategic Framework* (2024) 7. Available at: https://www.geostrategy.org.uk/research/foreign-interference-in-democratic-societies/

The Legal Architecture: Balancing Privacy and Security

The evolution of hostile state actors has fundamentally reframed the legal debate over how to balance individual privacy with collective security. British courts and lawmakers have been tasked with calibrating the boundary between liberty and security in the age of hybrid warfare and cyber espionage.

The ECHR Framework

Article 8(1[5]*)* of the ECHR guarantees the right to respect for private and family life, home, and correspondence. However, it is a qualified right. Under *Article 8(2)*[6], interferences are permissible where they:

1. Are "in accordance with the law," requiring clarity, foreseeability, and safeguards against abuse;
2. Pursue a legitimate aim, such as national security;
3. Are necessary in a democratic society; and
4. Are proportionate to the aim pursued.

As articulated in *Sunday Times v United Kingdom (1979) 2 EHRR 245, §49,* "in accordance with the law"[7] demands that laws be accessible and foreseeable. The principle of necessity, as confirmed in *Handyside v United Kingdom (1976) 1 EHRR 737, §48*, requires that any interference corresponds to a "pressing social need"[8] and employs the least intrusive measures necessary to achieve its legitimate aim.

Equally, *Article 2* imposes a positive obligation on states to protect life. Though *Osman v United Kingdom* arose from a domestic policing context, its principle applies no less persuasively to national security. When intelligence agencies become aware of threats to life, they are obliged to act[9]. Thus, the United Kingdom's security services operate under a permanent legal tension: failing to deploy surveillance powers may breach *Article 2*, while excessive intrusion risks violating *Article 8.*

Legislative Reform

The ECtHR has subjected British surveillance practices to rigorous scrutiny. In *Big Brother Watch and Others v United Kingdom,* the Court held that bulk interception is not inherently unlawful. However, it cautioned that:

[5] European Convention on Human Rights, Article 8(1).
[6] European Convention on Human Rights, Article 8(2).
[7] *Sunday Times v United Kingdom* (1979) 2 EHRR 245, [49].
[8] *Handyside v United Kingdom* (1976) 1 EHRR 737, [48].
[9] O*sman v United Kingdom* (1998) 29 EHRR 245, [115].

"A measure cannot be regarded as necessary in a democratic society if it does not correspond to a pressing social need, and if the reasons adduced by the national authorities to justify it are not relevant and sufficient" [§387].[10]

Critically, the ECtHR acknowledged "the multitude of threats States face in modern society"[11] and affirmed that bulk interception, if accompanied by robust safeguards, does not violate the ECHR. The deficiencies it identified, such as the lack of independent approval for bulk warrants and inadequate protections for journalistic material, largely concerned the legacy system under the *Regulation of Investigatory Powers Act 2000*, much of which has since been overhauled.

Similarly, in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (C-623/17), the Court of Justice of the European Union ruled that general and indiscriminate transmission of traffic and location data to security agencies, even for national security purposes, exceeded what was "strictly necessary"[12] and breached Articles 7, 8 and 11 of the Charter of Fundamental Rights.[13]While this decision applied to the UK pre-Brexit, it continues to shape surveillance standards through its influence on EU–UK data adequacy agreements. However, the judgment did not prohibit targeted surveillance, nor did it suggest that bulk powers are inherently unlawful. It simply stated that interference in privacy must be bounded by strict necessity and proportionality. The UK's subsequent reforms, particularly the *Investigatory Powers Act 2016*, with its double-lock system[14] and independent oversight mechanisms, reflect a measured response to these concerns. Though subject to ongoing scrutiny, this framework shows that the UK has taken active steps to strike a balance between protecting national security and safeguarding individual rights, even amid evolving threats.[15]

The Investigatory Powers Act 2016

In response to these judgments, the United Kingdom enacted substantial reforms. The Investigatory Powers Act 2016 (IPA) replaced the fragmented RIPA regime and introduced a modernised legal framework for surveillance. Under *section 23 IPA*, the most intrusive warrants require both ministerial authorisation and approval by a Judicial Commissioner; a current or former High Court judge. This "double-lock" system ensures that surveillance powers are subject to both political accountability and independent legal scrutiny.

[10] *Big Brother Watch and Others v United Kingdom* (2021) App Nos 58170/13, 62322/14 and 24960/15, [2021] ECHR 439, [387].
[11] *ig Brother Watch and Others v United Kingdom* (2021) App Nos 58170/13, 62322/14 and 24960/15, [2021] ECHR 439, [424]
[12] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (Case C-623/17) EU:C:2020:790, [2020] 3 CMLR 27, [77].
[13] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (C-623/17) EU:C:2020:790, [2021] 1 WLR 4421, paras 69–82.
[14] Investigatory Powers Act 2016, ss 23, 138.
[15] Regulation (EU) 2016/679 (General Data Protection Regulation), art 45; see also *Investigatory Powers Act 2016*, ss.23, 138.

While the IPA preserves the possibility of bulk data collection, it imposes stringent safeguards. Warrants under *section 138* must specify operational purposes, and subsequent searches of collected data require separate authorisation. The Investigatory Powers Commissioner's Office (IPCO) performs audits and reviews to ensure lawful use of powers. The Investigatory Powers Tribunal (IPT) offers an independent judicial forum for complaints regarding misuse of surveillance powers. The ECtHR's ruling in *Big Brother Watch* prompted further changes. The government introduced requirements for internal authorisation before analysts can request intercepted data using strong selectors, such as email addresses, and assured judicial approval when searches could involve confidential material. These reforms directly address Strasbourg's concerns and affirm the UK's commitment to proportionality and oversight.

National Security Act 2023

The National Security Act 2023 further underscores the evolution of Britain's legal architecture. It introduces new offences for espionage and foreign interference[16], reflecting the government's recognition that threats now extend far beyond terrorism into the realms of hostile-state activity, cyber operations, and disinformation campaigns.

Reconciling National Security with Democratic Freedoms

These legal protections are not mere formalities; they are the hallmarks of democratic governance. As Andrew Parker, former Director-General of MI5, asserted:

"We do not, and could not, go browsing at will through the lives of innocent people."[17]

Yet the realities of modern national security require capabilities robust enough to counter sophisticated adversaries. Hostile-state actors use tactics deliberately designed to evade traditional investigative methods. Connections between individuals, organisations, and hostile operations often surface only through analysis of large datasets. The NSS's acknowledgment of technology as both a vulnerability and a defensive tool demonstrates why such capabilities, though powerful, remain necessary, so long as they are carefully constrained.

Necessity, however, cannot surpass proportionality. Surveillance measures must be lawful, targeted, and subject to independent oversight. A clear illustration of this balancing exercise is found in *Bridges*

[16] National Security Act 2023, ss 13–15.
[17] Andrew Parker, Director-General of MI5, Speech at the Royal United Services Institute (RUSI), *The Balance Between Security and Privacy in the Digital Age* (25 January 2016).

v Chief Constable of South Wales Police [2020] EWCA Civ 1058, where the Court of Appeal held that the police's deployment of live facial recognition technology engaged *Article 8* rights and required careful legal justification[18]. The Court ruled the deployment unlawful, owing to inadequate safeguards and policy clarity, yet crucially declined to outlaw the technology altogether. Instead, it affirmed that new surveillance tools can remain compatible with fundamental rights if subject to rigorous assessments. This case demonstrates how UK law evolves to address novel technologies without sacrificing core democratic principles. As Klass affirmed, states enjoy a margin of appreciation in national security, but that margin is not unlimited. Courts remain vigilant to ensure the "very essence of the right"[19] to privacy is preserved.

Conclusion

The United Kingdom has forged a legal and institutional framework that, in principle, strikes a lawful and proportionate balance between national security and individual privacy. The Investigatory Powers Act 2016, the National Security Act 2023, and robust judicial oversight mechanisms demonstrate the state's determination to uphold this equilibrium.

Nonetheless, the balance is not fixed. It must be continuously recalibrated in light of technological developments, judicial scrutiny, and the ingenuity of hostile actors. It is submitted that the United Kingdom has largely achieved the delicate balance between liberty and security. The evolution of its legal framework, and the state's responsiveness to judicial guidance, attest to a system of checks and balances that, while imperfect, is fundamentally working. In doing so, the United Kingdom continues to heed the warning in *Klass*: that even in confronting grave threats, a democracy must not become the tyranny it seeks to avert.

[18] *Bridges v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 WLR 5037.
[19] *Klass and Others v Germany* (1978) 2 EHRR 214, §49.

Bibliography

Cases

- Big Brother Watch and Others v UK (2021) App. Nos. 58170/13 et al, §387
- Bridges v Chief Constable of South Wales Police [2020] EWCA Civ 1058
- Handyside v UK (1976) 1 EHRR 737
- Klass v Germany (1978) 2 EHRR 214
- Leander v Sweden (1987) 9 EHRR 433
- Malone v UK (1985) 7 EHRR 14
- Osman v UK (1998) 29 EHRR 245
- Privacy International v Secretary of State for Foreign & Commonwealth Affairs (C-623/17) (Grand Chamber)

Legislation

- Investigatory Powers Act 2016
- National Security Act 2023

European Treaties

- European Convention on Human Rights, Articles 2, 8, 10
- Directive 2002/58/EC (Privacy and Electronic Communications Directive), Article 15(1)
- Charter of Fundamental Rights of the EU, Articles 7, 8, 11

Contextual Materials

- HM Government, *National Security Strategy* (London, June 2025)
- Council on Geostrategy, *Foreign Interference Report* (2024) – Dr John Hemmings
- Interview with Andrew Parker, former Director-General of MI5 (2023)