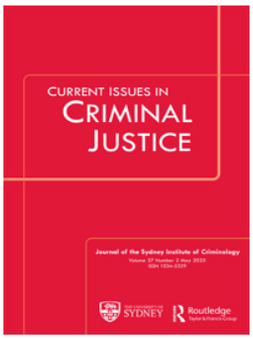

Routledge
Taylor & Francis Group

Current Issues in Criminal Justice

ISSN: 1034-5329 (Print) 2206-9542 (Online) Journal homepage: www.tandfonline.com/journals/rcic20

Sensitive research & anti-money laundering: a possible marriage of convenience?

Brendan Walker-Munro, Jamie Ferrill & Milind Tiwari

To cite this article: Brendan Walker-Munro, Jamie Ferrill & Milind Tiwari (2025) Sensitive research & anti-money laundering: a possible marriage of convenience?, Current Issues in Criminal Justice, 37:2, 308-333, DOI: 10.1080/10345329.2025.2467483

To link to this article: https://doi.org/10.1080/10345329.2025.2467483

Published online: 24 Mar 2025.

CURRENT ISSUES IN CRIMINAL JUSTICE
2025, VOL. 37, NO. 2, 308–333
https://doi.org/10.1080/10345329.2025.2467483

Routledge
Taylor & Francis Group

Sensitive research & anti-money laundering: a possible marriage of convenience?*

Brendan Walker-Munro [a], Jamie Ferrill [b] and Milind Tiwari [b]

[a]Faculty of Business, Law & The Arts, Southern Cross University, Bilinga, Australia; [b]Australian Graduate School of Policing and Security, Charles Sturt University, Bathurst, Australia

ABSTRACT

Nation-states are increasingly turning to the use of espionage and foreign interference to further their programmes of technology acquisition. This threat is especially prevalent where sensitive, technological, and innovative research is taking place—namely our universities and higher education institutions. To prevent the diffusion of technological knowledge against the national interest, Western nations are erecting bulwarks against illicit technology transfers, consisting of both legal and policy frameworks with varying degrees of success. In that context, this paper has two aims. The first is to expose an under-theorised area of legal research. The second aim is to explore a novel regulatory mechanism—adapted from the existing anti-money laundering regime—that could both enhance the current anti-money laundering regime and be applied to sensitive and dual-use research, with a view to providing a robust and matured response to foreign interference and espionage by international threat actors.

ARTICLE HISTORY
Received 31 May 2024
Accepted 11 February 2025

KEYWORDS
Sensitive research; AML; money laundering; national security; higher education.

Part I: introduction

Clark Kerr (1995, p. 194) once famously coined, 'As society goes, so goes the university; but also, as the university goes, so goes society'. The notion of the university as a microcosm of our social and cultural lives has a lengthy history: they have been centres of invention and creativity, criticism and revolution (Hare, 2023). Within those institutions, the notion of 'academic freedom'—that an appointee of the university may engage in public debate on *any* topic within their area of expertise, no matter how controversial or inflammatory—has received qualified legal protection by the High Court of Australia's decision in *Ridd* (2021).[1] It implies a right to free inquiry within the academic institution, but also an obligation to preserve the institution as a site where freedom of inquiry is encouraged and practiced without interference or censorship (Butler, 2017).

CONTACT Brendan Walker-Munro brendan.walker-munro@scu.edu.au

*The authors received no financial support for the research or authorship of this work outside that provided by their employer or institution, and the arguments and comments made in this article are the author's alone and neither involve or imply endorsement by the author's employer or institution.

But universities are also coming under increasing pressure from a largely unexpected quarter. States all over the world are ramping up their efforts to infiltrate, undermine and even exploit university-based research or exert influence on campuses to achieve their foreign policy objectives (Parliamentary Joint Committee on Intelligence and Security, 2022). Attempts to limit or eliminate such threats usually involve clamping down on sensitive knowledge, information, or technologies—measures which run up against scholarly values of transparency, cooperation and collaboration (Thomson, 2023). At the same time, many universities rely (at least in part) on the monetary value of their research outputs, whether in the form of patents or other intellectual property, or the funding inputs which drive innovative research (Hartman, 2010, pp. 70–71). Not only can national security restrictions have implications for a university's reputation, but they may also threaten its financial liquidity or social licence to operate.

Yet the risks of not taking action are catastrophic. Duke University Professor David Smith was entirely unaware when he hired ambitious young postdoc researcher Ruopeng Liu. In 2005, Liu would go on to allegedly steal metamaterials research being conducted at Duke (McFadden et al., 2018). In 2021, the Australian Parliamentary Committee on Intelligence and Security (PJCIS) warned in its inquiry report that the contributions of some universities in Australia were openly being exploited by foreign intelligence agents. Then in 2023, the Director-General of ASIO warned that academic staff were being targeted by intelligence officers for potential compromise when attending international conferences (Burgess, 2023). China might dominate the headlines (Lewis, 2017; Rechtschaffen, 2020; Siddiqui, 2023); but Russia and North Korea have continued their efforts in illicit technology collection (Greene, 2022; Burakovsky, 2022), whilst states which are notionally allied to Western interests—such as Saudi Arabia (Mervis, 2019; Bernstein et al., 2019) and Israel (Bamford, 2023)—continue to exert their influence on foreign universities. The US has even gone so far as to schedule fake academic conferences staffed by CIA agents to lure Iranian nuclear scientists to defect to the West (Golden, 2018).

Calculating an appropriate balance between openness and secrecy, trust and scepticism, and protection versus collaboration has never been more difficult: 'the enemy has become less targetable, the technology more difficult to define (as it is continually emerging), the university more global and more sensitive to commercial interests, and that enforcing any kind of control is now an international, not national, matter' (Evans & Valdivia, 2012, p. 178). The emerging literature describes the notion of 'research security', which involves protecting the nature of research endeavours, and the researchers themselves from access, interference, or unwanted manipulation (Government of Canada, 2023; Government of the Netherlands, 2023). Though states have achieved varying levels of maturity in research or knowledge security frameworks, the actual 'doing' of institutional governance remains largely undertheorized. This paper intends to bridge the gaps in the literature by proposing novel regulatory mechanisms for universities, borrowed from the anti-money laundering and counterterrorism financing (AML/CTF) environment. The AML/CTF regime has been important in harmonising laws and institutions and has received global political support (Levi et al., 2018). AML/CTF regimes are designed to control attempts by criminal actors to clean the source of illegally obtained funds, by which they either disguise the origin of such funds or falsely attribute the income to some legitimate source, or both (Strange, 1998,

p. 25). The word 'control' here is deliberate; no regime will unequivocally stop the nefarious acts, but they can indeed aid in the control of them. Although AML and CTF regimes share structural analogies such as encouraging intelligence sharing and compliance monitoring across law enforcement, intelligence services and private institutions (Chadderton & Norton, 2019), CTF is often referred to as involving 'reverse money laundering' (Cassella, 2004) or 'redundant fragmentation' (King & Walker, 2015), or even 'not laundering at all' (Van Duyne et al., 2018a, vii). Since the rise of terrorism post-9/11, AML controls (along with sanctions) are also increasingly utilised with a national security nexus—often involving a number of precautionary controls designed to detect and control illicit activity (Saravalle, 2022). This doesn't imply that the current system is flawless. However, by undertaking this exercise in regulatory comparison and development, we can propose ways to enhance the well-established AML/CTF regime, and, by leveraging its foundational strengths, create a research security framework.

We intend to identify unique methodological similarities between controlling money laundering and securing universities' research processes, which make an adaptation of the regulatory regime so attractive. Part II will provide a brief background to both research security and AML/CTF regulation before Part III examines and evaluates the AML/CTF regime in Australia. Part IV proposes a new research security regime which borrows from and adapts certain AML controls for application in a university context. Finally, we aim in Part V, VI and VII to achieve two objectives: first, by contributing to a nascent academic discourse on the nature of regulating science and knowledge production in universities, and secondly, to make a series of novel but modest law reforms which could achieve an appropriate balance between securing sensitive research and protecting openness, transparency and freedoms of expression.

Part II: background

Due to the rise of cross-border drug trafficking in the US during the 1970s and 1980s, an international legal framework to combat money laundering emerged. This framework operated under the principle that targeting the financial gains from such illicit activities represents the most effective strategy against expansive, multinational criminal enterprises (Alexander, 2007). In 1988, the international AML regime gained traction through the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (United Nations, 1988). Then, in 1989, the Financial Action Task Force (FATF) was established by the Group of Seven (G7) to examine and develop measures to combat money laundering (FATF, 2024). With the establishment of the FATF in Paris in 1989, global AML norms and standards were born with the initial 1990 '40 Recommendations'. Following the 9/11 terrorist attack in the US, the FATF expanded its mandate to counter-terrorism financing, adding 9 Special Recommendations. The next and current iteration which also includes proliferation financing (PF) recommendations is again known as the FATF Recommendations, with CTF and PF comprehensively included.

The FATF was not initially set up to be the global standard-setting body for AML/CTF regimes, nor were AML initiatives developed alongside any measures of effectiveness or even efficiency (Levi et al., 2018). The 40 Recommendations were initially presented as recommendations for countries on measures to be adopted to prevent money laundering

in their financial systems (de Koker, 2022). Over the years, these recommendations have emerged globally as the benchmark for AML/CTF efforts. They encompass aspects such as criminalisation of money laundering and terrorist financing, establishment of financial intelligence units (FIUs), and ensuring compliance with customer due diligence and other AML/CTF measures (APGML, 2024), underpinned by a risk-based approach. This transformation from a task force issuing recommendations to becoming a global standard-setting body (i.e., one no longer operating on a time-bound mandate) underscores the growing complexity of financial crimes and the need for a coordinated international response.

Research has supported the notion that compliance with FATF standards correlates with reduced money laundering risks (Manning et al., 2021). However, it has also been challenged, with researchers questioning if adherence to the standards set out by the FATF actually prevents serious crime (Chaikin, 2009; Pol, 2018). For instance, while the UK's money laundering legislation was considered comprehensive in terms of the offences it covered and the standard of proof required (Aurasu & Rahman, 2018, p. 107; Herlin-Karnell, 2017), entities incorporated in the UK were still involved in laundering billions of dollars of illicit funds (Tiwari et al., 2023). This outlines the inherent limitations of the AML/CTF regime. Still, we cannot possibly know the counterfactual; that is, how much illicit money would or could be laundered without the current controls in place.

One of the challenges or limitations is that compliance with AML/CTF regulations imposes operational costs and complicates the functioning of the financial services sector, thereby reducing its efficiency (Naheem, 2020). Furthermore, lack of clarity surrounding data access and processing of personal information raises concerns around privacy (Alberto, 2016). The lack of clear definition around key concepts, such as 'suspicious activity' in the UK's AML regulations, can result in over-reporting, further complicating the already intricate regulatory landscape (Norton, 2018). The problem is exacerbated further by prevailing differences in defining offences and penalties across jurisdictions, which undermine the overall effectiveness of the AML/CTF regime (Tiwari et al., 2020).

While there is no reliable independent measure of 'effectiveness' *per se*, these challenges can actually be beneficial when designing a new regime. In the transnational security space (Jakobi, 2018)—where both AML/CTF and research/knowledge security coexist—we can rationalise what works and indeed what does not work to create a more effective system. That is, by learning from the mistakes of the former, we are better positioned to design a system with the fundamentals intact, but with more effective connections between the aims and means. Iteratively, this also enables reflection on the current AML/CTF regime and may indeed help to strengthen it vis-à-vis the recommendations that emerge.

One of the FATF's main tools for compelling effective use of its standards is the Mutual Evaluation Report (MER) process, which relies on peer reviews to assess countries' level of compliance with the FATF Recommendations (Pisa, 2019). The goal is to ensure that adequate response mechanisms are implemented to combat emerging threats in the financial system in each country (Sansonetti, 2000). Such mutual evaluations provide an opportunity for the FATF to review its standards and guidance documents to assess and improve upon the provided recommendations for access to reliable and accurate information (Transparency International, 2019).

The MER process, while not perfect, does bring to the foreground deficiencies in member countries' AML/CTF regimes. For example, the last MER completed in Australia in 2015 found the country to be non-compliant with recommendations 8 (related to non-profit organisations), 13 (correspondent banking), 22 (DNFBPs: Customer due diligence), 23 (DNFBPs: Other measures), 25 (Transparency and beneficial ownership of legal arrangements), and 28 (Regulation and supervision of DNFBPs). As a result, it was placed on enhanced review. As per the most recent review in March 2024, Australia is still non-compliant with recommendations 22, 23, 25, and 28 along with being only partially compliant on 6 additional recommendations 1, 15, 16, 24, 27, 35 (FATF, 2024).

While the FATF has no power under international or domestic laws to compel compliance, it does have coercive actions available such as 'grey-listing', which can result in limited foreign investment and impediments to obtaining credit. On the one hand, these coercive powers can compel governments to ensure their regimes meet the minimum standards, however, in the case of developing countries, the consequences can be more dire (de Koker et al., 2023, p. 81). To improve, the FATF approach could reassess its listing approach to prioritise significant financial sectors, address unintended consequences, support sustainable resourcing for smaller economies, and extend observation periods to prevent unnecessary economic harm from premature greylisting (de Koker, 2024).

From the Australian perspective, the Australian Government passed the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) in response to the global concern around money laundering and terrorist financing (Ross & Hannan, 2007). The AML/CTF Act is administered by the Australian Transaction Reports and Analysis Centre (AUSTRAC): Australia's FIU and regulator. The initial AML/CTF Act included 'high-risk' sectors as part of Tranche I: financial institutions, cash-carrying services, bullion dealers, casinos, remittance service providers, and stored value card providers (Sathye & Islam, 2011).

Soon after its initial implementation in 2006, the government began discussions about reforming the AML/CTF Act, known as Tranche II reforms, in order to meet international commitments. In line with the FATF recommendations, the reforms would bring a range of entities or individuals operating outside the traditional financial system but at risk of being exploited for money laundering and terrorist financing under the AML/CTF Act. Known as designated non-financial businesses and professions (DNFBPS), these entities or individuals include real estate agents, lawyers, accountants, dealers in precious metals and stones, and trust and company service providers. Australia only passed the Tranche II reforms on 10 December 2024, when it passed the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024. The security implications of this inaction have not gone unnoticed (Legal and Constitutional Affairs References Committee, 2022).

The AML/CTF regime has been implemented across the Tranche I sectors in Australia, resulting in a highly regulated financial sector, which has matured and achieved many of its regulatory objectives (Norton, 2017); however, money laundering remains a significant challenge in a number of other regulated industries (Langdale, 2023). Others have suggested that the true effectiveness in Australia's AML framework actually derives from its aggressive pursuit of taxes (Chaikin, 2018), or its civil confiscation scheme which—like the United Kingdom—relies upon a legal threshold of reasonable suspicion

(Goldbarsht, 2023). Further, compliance in the financial services has not come without a cost, with numerous participants claiming both start-up and ongoing compliance costs in the many millions of dollars, which in turn has increased consumer costs for access to banking and financial services (Sathye, 2008; Van Duyne et al., 2018a). The glacially slow speed of the Australian Parliament to pass Tranche II reforms has also been criticised as permitting national security threats to embed and/or enrich themselves ahead of formal reporting obligations coming into force (Goldbarsht & Benson, 2024, p. 797; Scott & Webster, 2024).

Those criticisms aside, the AML/CTF regime poses a strong security governance option for establishing and maintaining a cross-border security network. The AML/CTF regime frames illicit finance as a global security risk, requiring a comprehensive approach to combat diverse unlawful activities and emphasising public-private collaboration activities (Jakobi, 2018). This is precisely the form that enacted mechanisms for many forms of research security regulation have taken in those jurisdictions which have grappled with the problem (Government of Canada, 2023; Government of the Netherlands, 2023). This use of the AML/CTF regime to enhance security in other settings has also been under-researched, hence the focus of this work.

Research security is a similar field of endeavour which seeks to protect intellectual and commercial knowledge from interference, espionage and illicit or quasi-illicit transfers. Research security first emerged in the context of the post-World War II United States and Canada, where the ongoing Cold War required numerous layers of defence against espionage and theft of important scientific discoveries (especially nuclear secrets; Wilner et al., 2022, p. 28). Rather than confront the overwhelming military force displayed by Russia up until the collapse of the Soviet Union, the US and Canada focused on retaining their technological advantage, establishing incredibly robust export control regimes which prohibited export of almost all military technologies (Daniels & Krige, 2022). Despite attempts by George Bush and Barack Obama to deregulate US export control (particularly the much-maligned International Traffic in Arms Regulations or ITAR), US export controls remain some of the strictest in the world (Tomoshige, 2022). Canadian law largely followed suit, and developed characteristics that survived the end of the Cold War and reinstitution of trade between East and West (National Research Council of the National Academies, 2009).

The decline of Russia and the rise of China as strategic adversaries, coupled with the twinned increase in private investment in university research and development and growth in degree-qualified positions, fuelled a spike in industrial espionage and intellectual property theft (even amongst allied nations: Malakoff, 1999, p. 882). Legal and policy responses began to evolve, with US and Canadian export control laws amended to 'deem' the sharing of knowledge to be an export of the relevant technology if 'the same transfer to the most recent country of citizenship or permanent residency of the foreign national would require a license' (Kerr & Casey, 2021, p. 7). The National Science Foundation (NSF) subsequently issued policy guidance required to be followed by universities which sought government funding, and President Trump issued a Presidential Directive which required universities to take due diligence steps in cooperating with foreign entities (Trump, 2021). Canada followed suit shortly after, publishing a 'Policy on Sensitive Technology Research and Affiliations of Concern' (Government of Canada, 2024a). This policy—applicable at all federally funded Canadian institutions—limits cooperation in

'Sensitive Technology Research Areas' or with 'Named Research Organisations' who pose national security threats (Government of Canada, 2024b, 2024c).

At the same time, the United Kingdom began its foray into development of a 'trusted research' paradigm (UKRI, 2024), building on US efforts to stem secrets being illicitly exported to countries of concern. Under the *National Security and Investment Act 2021* (UK), acquisitions of entities working on any of 17 knowledge areas—such as advanced robotics, nuclear power, quantum, satellite or space technologies, and cryptography—must notify the Home Office and seek approval (*National Security and Investment Act 2021* (UK), sections 6(2) and 8(2), (5) and (6).). The Secretary of State also possesses the power to 'call-in' acquisitions which the Secretary reasonably believes would or could involve investment in those fields. More recently, the *National Security Act 2023* (UK) has created a foreign activities and foreign influence registration scheme. The purpose of this scheme is to require UK entities (including universities) to publicly register 'foreign influence' and 'foreign activities' where persons in the UK are acting on instructions of foreign governments or their officials (*National Security Act 2023* (UK), sections 65 and 69). Universities are not exempt from this reporting obligation, and the interplay between the Acts serves as a vital reminder of the precarious balance between the protection of Western democratic ideals and the national security apparatus designed to detect, identify and mitigate threats against itself (Scott, 2023).

The history of the Netherlands' response to security threats to university research in the face of illicit technology thefts and transfers is far newer. Freedom in educational settings is a Dutch constitutional right, enshrined in its various campuses spread around the country with centuries of shared history between them (Cohen & van der Steege, 1982, p. 274). During the Cold War and its immediate aftermath, the *Academische Raad* (Netherlands Universities' Council) further acted by fiat to promote 'efficient co-operation between the universities and the adaptation of university education to the development of science and to the requirements of society' (275).

That approach changed drastically as a result of the 'Fouchier affair', where Dr Ron Fouchier sought to publish a paper showing 'a lab-created H5N1 flu strain could infect ferrets via airborne transmission' (Enserink, 2015). The US National Science Advisory Board for Biosecurity recommended Fouchier retract the publication, but then the Dutch government intervened, demanding Fouchier obtain an export control licence prior to the paper being made public (Council of the European Union, 2009). Even though Fouchier did so, Erasmus MC—his employer—sued the Dutch government for imposing the licence requirement. Both Fouchier and Erasmus MC lost at first instance (*X established in Z v Minister for Foreign Trade and Development Cooperation,* 2013). On appeal, the Amsterdam Court of Appeal overturned the ruling, but only so much as they stated that neither Fouchier nor Erasmus MC had standing to sue the government. This was because Fouchier had already obtained the permit, and used it to publish his results, so there was no legal remedy which the Court of Appeal could give (*X to Z v Minister for Foreign Trade and Development Cooperation,* 2015).

Following Fouchier's run-in with Dutch export control regulations, there were more issues raised that suggested drastic action needed to be taken. In 2020, Chinese tech company Huawei established an AI research project with the University of Amsterdam (UvA) and the Free University of Amsterdam (VU) called DREAMS Lab, even after Huawei had been banned from providing 5G technology in the Netherlands because of

national security concerns (Snetselaar, 2022). Following these events, Minister van Engelshoven wrote a letter to Dutch Parliament in November 2020, where he outlined a package of measures to safeguard research security (Rijksoverheid, 2020). This was immediately followed by the Association of Dutch Universities publishing a framework in the following July (VSNU, 2021), followed by the establishment of a 'National Contact Point for Knowledge Security' (Rijksoverheid, 2023). The Dutch approach to research security is somewhat unique as it involves a far closer cooperation between government and intelligence services (such as the Netherlands General Intelligence and Security Service; 'AIVD') than occurs in other Western nations. That said, recent steps by the Dutch government to introduce the *Wet voor het Toetsingskader ongewenste kennis- en technologieoverdracht* [Screening Act for Undesirable Knowledge and Technology Transfer] have been met with strong condemnation (Wassink, 2023; KNAW, 2023; Upton, 2023).

Research security is a construct intended to confront the dangers of unrestricted and unmonitored collaboration with foreign entities that pose risks with national security dimensions. Whether the source of the risk is the host government of the foreign entity, or certain actors or vectors within the entity itself, the imposition of controls for research and knowledge security purposes essentially seeks to restrict the use of institutional knowledge to legitimate, peaceful scientific endeavours. In this way, research and knowledge security have much in common with AML/CTF regimes: the purpose of both regimes is to transparently prevent illicit uses of a resource (knowledge vs money) without impacting or constraining licit uses of that same resource (which make up the bulk of transactions), and protect against threats with a national security dimension (i.e., spies, terrorists, money launderers).

Part III: identifying AML/CTF principles relevant to research security

Enrolment and registration with austrac

Reporting Entities (REs) as specified under section 6 of Australia's AML/CTF Act are required to register with AUSTRAC. Registration places several obligations on these REs to control serious financial crime. These include developing an AML/CTF programme, reporting certain transactions and suspicious matters, submitting regular compliance reports, keeping records (e.g., transactions, electronic fund transfers, customer identification procedures, and regarding the AML/CTF programme), informing AUSTRAC of any changes to enrolment details, and in some cases paying an industry contribution levy (AUSTRAC, 2024a). Remittance service providers and digital currency exchanges have additional obligations, demonstrating the adaptability of these programmes based on the context of the risk.

Developing an AML/CTF program

One of the obligations for REs is the need for a risk-based AML/CTF programme, which outlines how obligations under the AML/CTF Act will be met (AUSTRAC, 2024b). Risk-based assessments in AML are generally calculated by reference to the relationship between observable phenomena and the risk being quantified, the potential seriousness of risks being watched for, and vulnerability of the sector to those risks (Ross & Hannan, 2007, pp. 110–111; Dalla Pellegrina & Masciandaro, 2009). Further, such risk-based

AML/CTF programmes must adhere to subordinate regulations under the AML/CTF Act and must 'have regard to the nature, size and complexity of its business and the type of ML/TF risk that it might reasonably face'.[2] Special AML/CTF programmes also exist but are applied uniquely to holders of Australian financial services licences who receive designated services under the AML/CTF Act.

Standard AML/CTF programmes consist of Part A (i.e., 'general') and Part B (i.e., 'customer identification') (AML/CTF Act, section 84(1)(b)). Part A includes a number of core elements all REs must have in place (AML/CTF Rules, Parts 8.2-8.7):

- regularly reviewed risk assessments,
- oversight by a Board/CEO/equivalent,
- having an AML/CTF compliance officer,
- engaging in employee due diligence and risk awareness training programmes,
- integration of regulatory guidance from AUSTRAC; and
- Ongoing customer due diligence (OCDD) systems and controls in place.

Part B then focuses on the specific risks and the operating context of REs. In other words, Part B involves more customised risk management strategies, enhanced customer due diligence (ECDD) procedures, and protocols for beneficial owners and politically exposed persons (PEPs).

Screening of politically exposed persons ('PEP')

PEPs, as defined upon the coining of the term by the Basel Committee on Banking Supervision (2001, p. 10), are 'individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials'. Since formally being recognised, the concept of PEPs has been included throughout both domestic and international AML/CTF regimes including the FATF Recommendations, the EU AML Directives, both Canada and the United States AML/CTF regulations and legislation, and Australia's AML/CTF Act and AUSTRAC AML/CTF programme requirements.

In the financial crime realm, there have been cases where corrupt PEPs use legal entities to obscure their identity; they are associated as the beneficial owner of the client, which distances them from illicit transactions (Canestri, 2019). For example, the 2016 Panama Papers, 2017 Paradise Papers, and 2021 Pandora Papers all exposed the names of several PEPs who used mechanisms including shell companies to obscure their financial activity: much of it illicit (ICIJ, 2024a, 2024b, 2024c). With wider links to corruption, this revelation demonstrates the threat to the rule of law and unique risks PEPs pose to the international financial system. With political power comes the risk of corruption; in this light, this means exploitation of positions of authority and trust to facilitate illicit activity, opportunities for embezzlement, links to organised crime to further illicit activities, and vulnerabilities to coercion.

Due to the higher risks they pose within the AML/CTF regime, noting there are varying levels of risk within this category, ECDD measures are required when dealing with PEPs. It is up to the RE to apply risk-based procedures to determine if customers

or beneficial owners are PEPs. In Australia, all foreign PEPs must be treated as high-risk customers. To assess domestic and international organisation PEPs, REs must use their risk-based procedures to determine where on the risk spectrum they sit (AUSTRAC, 2024b). From the identification stage, monitoring of PEPs ensues; this includes ECDD measures, ongoing monitoring, record keeping, training and awareness, and reporting obligations.

The Fintel Alliance

Controlling financial crime requires more than just technology or individual efforts; it demands cooperation, open dialogue, and a focus on real risks. Clear communication and trust are key to breaking down barriers and ensuring effective collaboration. Echoing the concept of networked policing (Ayling et al., 2006), integrating state and civil society resources to govern security lends itself to the financial crime space. That is, controlling (or 'policing') financial crime should not solely be the function of the state, but rather should be distributed across a network of actors, each contributing unique resources and capabilities (Grabosky, 2013). In the context of a financial crime-focused public-private partnership (PPP), the networked approach can work by integrating the expertise and capabilities of law enforcement, regulators, businesses, and other private entities. As governance shifts to more collaborative models, this creates opportunities to share resources, knowledge, and strategies more effectively (Maxwell & Artingstall, 2017). To this end, the Fintel Alliance (itself a PPP) was established by AUSTRAC in 2017 to enhance the financial sector's resilience to criminal exploitation and to support law enforcement in their investigations into national security and serious criminality (AUSTRAC, 2024b). Paul Jevtovic, the CEO of AUSTRAC at the time of the launch of the Fintel Alliance, stated 'the challenges this poses is by being the strongest that we can be. That strength is realised when industry and government agencies are actually working as one — as genuine partners, trusted partners'(Lynch, 2024).

As demonstrated by numerous states, PPPs can overcome information and intelligence coordination issues and have achieved significant impact in the fight against economic crime, demonstrating a range of benefits to both public and private sector members (Riondet, 2018). PPPs have resulted in an increase in the number of suspicious reports addressing particular threats, more timely and relevant reporting in response to active investigations or live incidents, improved quality and use of suspicious reporting and improved law enforcement outcomes supporting investigations, prosecutions, asset recovery, and other disruptions of criminal networks (Maxwell & Artingstall, 2017, pp. 20–21; Maxwell, 2019).

Despite their demonstrable benefits, PPPs are not without challenges of their own. For one, risk appetite across the membership affects attitudes towards sharing information; that is, in the practical sense, the more broadly information is disseminated, the greater the risk it could be misused (Chadderton & Norton, 2019). Private sector organisations may hesitate to share sensitive customer data due to fears of regulatory penalties or potential legal exposure, while government agencies may be cautious about sharing intelligence with the private sector, fearing misuse. It is essential to establish governance arrangements outlining how information shared within the PPP should be handled by REs, as well as how instances of regulatory non-compliance will be addressed. In a

similar vein, building trust despite sometimes paradoxical interests can cause tensions (Dudink et al., 2024). PPPs require long-term commitment and appropriate allocation of resources, both in terms of human and financial capital (Walker-Munro, 2021). However, many organisations, particularly smaller ones, struggle to justify diverting resources from their core activities to support PPP initiatives, even if the goals align with their interests. In turn, to ensure effectiveness, we have to overcome the enforced hybridity and power imbalances that can lead to significant resistance and inefficiencies, potentially undermining the success of collaborations aimed at tackling complex issues like financial crime and indeed research security (Dudink et al., 2024).

Part IV: adapting AML/CTF to research security

Educational institutions must evaluate their purpose and direction considering contemporary social, economic, and political challenges (James, 2012). Amidst these challenges, steps to safeguard the elements, methodologies, and outcomes integral to scientific research, inquiry, and discovery have become increasingly significant. Consequently, it is essential for researchers and universities to adhere to established norms comprising not only academic freedom, research integrity, excellence, openness, and ethics but also addressing the complex dynamics related to research and knowledge security (Shih, 2024).

Countries including China (Mallapaty, 2023), the United States (Trump, 2021), and the United Kingdom (NPSA, 2023) have implemented policies and regulations aimed at protecting their national scientific infrastructures from foreign control and appropriation; other countries are yet to follow with a similar approach. Despite the formulation and implementation of these policies and regulations, their effectiveness is subject to universities taking action (Lester et al., 2023). The current approach of research and academic institutions, including those in Australia, are insufficient, thus requiring a more assertive approach to address these challenges effectively.

The domestic AML/CTF regime provides a relatively sophisticated framework that is translatable into safeguarding research security. It provides an assertive approach through principles including Know Your Customer (KYC), Customer Due Diligence/Enhanced Due Diligence (CDD/ECDD), PEPs, transaction monitoring, information sharing, risk-based approaches, and evaluations. These principles are covered under REs' AML/CTF programmes (with the exception of mutual evaluations) and are captured under AUSTRAC's Part A and Part B programmes.

Consequently, the AML/CTF framework, as supported by the principles outlined in Part III, serves as a surveillance and risk management tool that can be adapted to enhance research security. For instance, tools like suspicious activity reports (SARs) and transaction monitoring mechanisms examine financial transactions and can detect early signs of illicit behaviour. The collected information can be explored for statistical analysis; however, if criminality is suspected, such information tends to serve as intelligence (Norton, 2018). Similarly, the AML/CTF framework employs a risk-based approach by emphasising the need to conduct ECDD where higher-risk entities such as PEPs or transactions from high-risk jurisdictions are involved (Gup & Beekarry, 2009). Furthermore, continual updating of client information and activities is required to ensure entities can continue to adopt risk-based assessments.

Therefore, adapting the AML/CTF regime to the context of research security would allow universities to implement an intelligence-driven and risk-based framework to address concerns of foreign interference, espionage, and intellectual property theft. However, such programmes would need to be administered by a sufficiently empowered and resourced regulator (some suggestions have been made that the Tertiary Education Quality and Standards Agency would be the natural home for this: PJCIS, 2022, p. 135) and would require Universities to implement the programmes accordingly.

Adapting Part A

As with Part A of the AML/CTF programme requirements (i.e., the core requirements, specified in section 84 of the 2006 Act) Part A of any research security programme should include risk assessments as the first component. This needs to be regularly reviewed and updated. Here, each RE (i.e., every university) has the onus of identifying any potential security risks associated with its research activities. This can range from intellectual property theft, access to sensitive information, insider threats, export control risks, and third-party risks with other universities, researchers, government agencies, industry partners, or foreign entities. A nuanced approach to what risk means and how it can be scaled for each organisation will need to be considered, given the challenges experienced in the AML/CTF regime.

Resourcing the division required for the research security programme will be a key factor. As within the AML/CTF regime, oversight of the programme is required. This can be sourced from the executive team: a Deputy Vice Chancellor or Chief Operating Officer would be suitable for this role. A research security compliance officer will also be required to be drawn from the managerial ranks. This responsibility could also be undertaken by the university's Office of General Counsel, who is also responsible for compliance.

Training and awareness amongst researchers and support staff at universities are also required as part of the programme's core requirements. This means regular training to educate anyone involved in research activities about their responsibilities in terms of safeguarding research assets. Training and awareness should also be integrated with both undergraduate and postgraduate student curricula to build broader identification capabilities. Despite the presence of regulations to strengthen research security on university campuses, such as in the US, these cannot replace initiatives by universities themselves (Lester et al., 2023). Therefore, it becomes pertinent on the part of these institutions to impart AML/CTF training, encompassing legal obligations, risk identification, and reporting procedures to their academic and administrative staff. This is essential to recognise and respond to threats affecting research security.

Next, systems and controls to ensure the research security reporting obligations are met will be crucial. In the AML/CTF space, reporting obligations include threshold transaction reports, international funds transfer instruction reports, SARs, cross-border movement reports (with a $10,000 threshold) and the requirements to produce AUSTRAC compliance reports when required. In the research security space, this provision could include the following obligations: reporting on new and existing international funding or collaborative agreements (including sharing of research data), incident reporting for suspicious actions or data breaches, compliance reports, research

security risk assessments, and third-party vendor reporting. For clarity, these provisions would need to work alongside (and not replicate) other limitations to research sharing such as export control and foreign investment laws. As a sector, universities already view themselves as over-regulated and under-resourced (Group of Eight, 2022) and so duplicative effort is unlikely to be accepted—yet they may be compelled to do so anyway.

Due diligence measureswould also be required. AML/CTF programmes already require ongoing transaction monitoring, as well as ongoing customer due diligence (OCDD) and enhanced customer due diligence (ECDD) as functions of risk-based programmes (AUSTRAC, 2024a). In the research security space, this transaction monitoring is relatively easy to implement. Applying mostly to bursaries, grants, or other financial benefits, it would involve identifying suspicious customer transactions that could be unusually large or from an unexpected source, transactions that stem from high-risk countries, transactions that are unusually complex, or those with a seemingly nefarious end-use, much like similar monitoring at financial institutions (Alkhalili et al., 2021). Another consideration is the susceptibility of students to become conduits for illicit funds owing to a lack of awareness, mirroring that of customers at financial institutions (Kiu & Leung, 2023). This can be considered in the transaction monitoring part of the programme. In terms of ECDD, these provisions have already been suggested to kick in when 'politically exposed researchers' (PERs, an adaptation of PEPs) interact with either high-risk entities (as determined via the risk-based approach), or what are determined to be 'prescribed foreign countries' (Walker-Munro, 2024b).

Finally, and perhaps most controversially, researchers could be subject to those same personal due diligence requirements (OCDD and ECDD) to identify internal risks. Despite the distinction between financial crime and research security, banks have long conducted due diligence on their employees (Mugarura, 2014), whilst academic institutions are only just beginning to embrace robust internal due diligence protocols. Such checks could be conducted by the internal risk or legal teams of universities, with a view to assessing the risks associated with collaborations on specific research projects or accepting funding which could be exploited by illicit actors. Furthermore, consistent with the emphasis placed on implementing a risk-based approach (Dalla Pellegrina and Masciandaro, 2009), universities might consider the use of this approach in line with principles of responsible internationalisation—the safe and secure practice of relationship building during our current era of degrading geopolitics (Shih, 2024).

Adapting Part B

Part B of the AML/CTF programme is focused on the principles and procedures surrounding KYC principles and beneficial owners, including PEPs (AUSTRAC, 2024b). The principles and procedures are tailored to the context of the organisation and its risks. This part of the programme includes an outline of the kind of information that needs to be collected and verified to ensure the university knows exactly whom they are dealing with. The measures to gather this information should also be included in this part of the programme. In the research security space, academic institutions should consider the implementation of comparable KYC procedures to verify sources of funds that encompass, but are not limited to, research grants, donations, payment of tuition fees and other university-related investment financial engagements to ensure

they are legitimate and not linked to illicit activities or entities. Leveraging technologies such as blockchain can aid in automating the KYC process (Moyano & Ross, 2017)—which is important for academic research institutions that deal with a diverse array of stakeholders and store a wide variety of data. This may form a core part of the programme, notably mitigating the 'cost of compliance' dilemma.

Part B would also include mitigation strategies for research-specific risks. These may include the higher-risk activities such as international collaboration, classified research projects, research involving dual-use goods, and so on. These will of course vary by department, research focus, and even university. Higher-risk entities such as PEPs would be included in this provision. Finally, implementing a regular review and audit of these measures is vital to examine their effectiveness and ensure that they are in line with latest regulatory developments and equipped to combat emerging risks.

Additional considerations

In alignment with the principles of responsible internationalisation and the AML/CTF framework, academic institutions ought to establish mechanisms for the exchange of information while fostering cross-border collaboration among research institutions. This could ensure that research security of academic institutions and universities remain intact given they are being actively targeted for hostile foreign activity (Wilner et al., 2022). Much of this responsibility could be encapsulated by Part A and Part B of the Research Security Programme, but the regulator would need to consider open yet secure channels for collaboration. Striking this balance would be the mark of mature research security management.

Further, by adopting the fundamental (i.e., networked policing model) properties of the Fintel Alliance, and building a government-led Research Security Alliance, institutions could be better equipped to tackle common threats. While inherently competitive in nature, just like any financial institution, developing a 'coopetition model' (Crick et al., 2024) to address shared research security concerns could be a promising path forward. This means collaboration across what might be considered industry 'rivals' for mutually beneficial outcomes: in this case, research security. It would require a fundamental shift in university consciousness in order to consider *both* individual performance and shared security priorities. Once established, the university-wide research security programme could benefit from FATF-style evaluations to assess compliance across universities, identify any weaknesses, encourage improvements, promote global standards (drawing on states with established research security programmes), and enhance transparency. However, FATF-style evaluations are not without their own weaknesses. Notionally, evaluations have been conducted in a manner that supports financial inclusion and the flexible use of simplified measures (Pisa, 2019); yet others suggest that 'financial exclusion can be exacerbated when the [risk assessment] is not correctly applied, especially if the FATF standards are not utilised in a proportionate manner based on existing risks' (Pavlidis, 2023, p. 3). Just like there has been inconsistency across REs themselves in applying a risk-based approach, there have also been inconsistencies across *assessors* regarding how threats arising from financial exclusion are treated (Van Duyne et al., 2018b). This suggests the need for a more systematic approach to evaluating these risks (Pisa, 2019). The systematic approach for risk assessment can be

applied within the research security space; by creating an evaluation framework with clear risk identification, assessment, prioritisation, and mitigation principles in place, review panels could effectively conduct periodic assessments of university compliance with the established standards. Impact and effectiveness assessment measures are also needed, and arguably lack in the AML/CTF regime (Nance, 2018).

Considering the aforementioned strategies to enhance research security, including those aimed at curbing illicit financial flows, it is essential to note that while fostering responsible internationalisation to ensure research security is of primary concern for universities, categorising research espionage and intellectual property theft entirely as institutional oversight, as has been the perspective in Australia, is misguided (Wilner et al., 2022). This includes appropriately funding research for universities such that they are not financially motivated to seek out high-risk ventures: some empirical evidence exists to suggest that even temporary shocks to federal funding drives universities to prioritise sources of private or anonymous funding (Babina et al., 2023).

In the absence of such balance, as exemplified by the critique of Australia's emerging approach to research security, there is a risk that such measures could be perceived to undermine the virtues of open science (Conley-Tyler & Law, 2020). Given the seemingly increasing prevalence of threats to universities (Walker-Munro, 2024a), there is an emerging need for a dynamic and robust response from academic institutions, along with responsible internationalisation on the part of researchers (Shih, 2024), to safeguard their integrity and contribute to global security efforts. This becomes even more critical in the context of rapid technological advancements, including the digitisation of the economy, which provides new avenues for illicit activities. Therefore, it is essential that current frameworks are revised and adapted to changes in technological evolution (Goldbarsht, 2023), incorporating principles from different institutional contexts, to ensure that research institutions and universities can maintain their integrity and contribute to global security efforts.

Part V: legal considerations

The infrastructure to adapt AML/CTF restrictions to research and knowledge security practices should not be considered a completely seamless and integrated solution. There are numerous legal provisions which would require amendments or reform to ensure the system operates in the manner intended and without adversely affecting the interests of all stakeholders. In some ways, the enactment of a research or knowledge security programme will require an inter-governmental approach similar to that adopted when the FATF recommendations were first implemented in Australia.

Establishing clear boundaries and ethical guidelines will be crucial when implementing research and knowledge security measures. For example, suspicious matter reports made to AUSTRAC under the AML/CTF Act are not admissible in court or tribunal proceedings, and persons who make such reports or handle AUSTRAC information cannot be compelled to reveal their contents (AML/CTF Act, sections 124 and 134). Information sought from REs by AUSTRAC for the purposes of administering reporting obligations cannot be used in any form of legal proceedings (save for alleged non-compliance) and equally treated with a high degree of secrecy (AML/CTF Act, sections 50A and 51). A similar standard of protection would need to be applied to research or knowledge security regimes to ensure that

information is not used for improper reasons (Walker-Munro, 2021) and universities are incentivised to speak freely in the interests of regulating the sector. Similarly, the results of due diligence checks (such as ECDD or OCDD processes) should not be permitted to be used by institutions as grounds for discrimination, where the nationality of the researcher or institution becomes a substitute for level of risk (Walker-Munro, 2021).

The institution of academic monitoring will likely also involve a significant resource impost, which universities cannot be expected to meet alone and should mark a point of deviation from comparison with AML regimes. Again, we turn to overseas to observe that many institutions involved in research and knowledge security leadership are integral to the host State government—the National Protective Security Authority in the UK, the National Security Foundation in the US, and Public Safety Canada in that country. Going a step further, the Netherlands National Contact Point is a collaboration centre external to but funded by the government, similar in some respects to the US National Science Advisory Board for Biosecurity (Patrone et al., 2012). Equally, technology may be able to play a greater part in screening and risk assessment by identifying higher risk cases for human intervention. The Australian National University (ANU) has recently commenced a trial of using artificial intelligence and data mining to scan its researchers' work for material which may be covered by Australia's *Defence Export Controls Act 2012* (Cth) (Group of Eight, 2021).

Research and knowledge security are also ethical minefields. Where individual researchers are not given adequate information, education, and incentives to disclose risky arrangements or ventures (not to mention protection for doing so), they bear the risk rather than sharing the risk with the hosting institutions. 'Bending' the rules can become commonplace, where applications are modified or tweaked to avoid words, language, topics or entities considered high-risk (Angell, 2000; Schünemann et al., 2015). Individual researchers may also (quite rightly) feel victimised for being the subject of harsh or draconian restrictions apparently based solely on their nationality, or the nationality of their research contemporaries (as was recognised in *Li v Canada*, 2023). Such cases may also motivate future foreign researchers and research entities to adapt or downplay what they disclose out of self-interest (irrespective of whether they are trying to engage in risky behaviours or not). In some unique circumstances, universities can also be placed in the unenviable position of having to choose between confidences it owes to researchers and the obligations they owe to government (Miller & Massoumi, 2015).

From an Australian perspective, the notion of research and knowledge security also abuts uncomfortably against the protections absorbed by 'academic freedom'; that is, the protections owed to academics to undertake both free and largely unfettered debate in public fora in 'the spirit of free inquiry' whilst also being free to participate and criticise university governance (French, 2019; Walker, 2020). Academic freedom also links to a wider freedom of expression founded in the *International Covenant of Civil and Political Rights*, whereupon '[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice' (United Nations, 1966). These rights have been buttressed in Australia by an implied constitutional right protecting freedom of expression in government or political matters (Stephenson, 2020).

However, such rights have always been subject to limitations founded on national security principles(Cosenza & Connors, 2004). As the High Court of Australia said,

'[t]he developed concept of intellectual freedom … has "always been delimited" by excluding, for instance, libel or efforts to incite violence' (*Ridd v JCU* 2021, [30]). Indeed, the *Ridd* court said that academic freedom is constrained in respect of 'legal' rights of others, such as rights not to be defamed, statutory duties not to reveal particular confidential information and not to reveal national security information (*Ridd v JCU* 2024, [24]-[26]). Research security could therefore fall well within a permissible class of infringements on the ordinarily wide freedom of academics and researchers to participate in public discourse.

Similarly, screening regimes would likely constitute a reasonable imposition on the privacy of individual researchers from a common law perspective should be explicitly dealt with in any future law reform. The implications for individual researcher and entity privacy—governed in Australia by the *Privacy Act 1988* (Cth)—would also need to be balanced against the need for sharing timely and accurate information between universities, funding bodies, government and industrial participants in the research endeavour. Scrutiny of individual researchers' work—and a potential to restrict and/or ban such work—could fly in the face of the hallowed traditions of other jurisdictions, where their constitutional guarantees might render Australia ineligible for research cooperation and collaboration (Karran & Mallinson, 2017). Screening in conjunction with researchers in such jurisdictions will need to be carefully handled—the extraterritorial reach of the *General Data Protection Regulation* is already well-known amongst national security researchers (Van der Sloot & Kosta, 2019).

If Australia were to adopt a research or knowledge security programme (administered by TEQSA or otherwise), it would be preferable to deal with such issues through the passage of legislation that protects academic freedom, alongside Australia's obligations under the ICCPR. Absent such a declaration in statute, we consider it highly likely—though unsatisfactory from a public policy perspective—that Australian courts would deem the above-mentioned limitations and safeguards as a reasonably necessary interference with the right to achieve the legitimate object of protecting national security.

The question of appropriate enforcement and sanction mechanisms also looms large in this discussion. Universities are historically respected institutions with a strong commercial and reputational incentive to comply with their legal, ethical and social obligations. They are also likely, like many other corporations of similar size and budget, capable of internally managing risks within certain thresholds. That said, banks and financial institutions frequently internally manage AML/CTF risk—with varying rates of 'success'—but do so alongside and in conjunction with external governmental supervision and monitoring. Universities in a research or knowledge security framework should be treated in an identical fashion.

Part VI: limitations in the current regime

The effectiveness of AML/CTF frameworks and their impact on the prevention and detection of illicit endeavours, including money laundering and terrorism financing, has been of interest to the academic community (Unger et al., 2014; Zavoli & King, 2021). We acknowledge the AML/CTF regime has limitations, as we have discussed throughout this paper. Still, research security programmes in Australia are nascent and under-developed—if they exist at all. Although all Australian universities have

endorsed the adoption of guidelines promulgated by the University Foreign Interference Taskforce (UFIT), the implementation of those guidelines is haphazard and *ad hoc* across the sector. Universities are also largely self-serving and self-regulatory in terms of risk analysis and management, with an absence of any form of monitoring or baseline compliance auditing. Amongst Australian funding bodies, only the Australian Research Council (ARC) has a framework in place for countering foreign interference—neither the National Health and Medical Research Council (NHMRC) nor the Commonwealth Science and Industry Research Organisation (CSIRO) have publicly referrable research security programmes in place. None provide specific guidelines or regulatory clarity around rules relating to research security.

AML/CTF practices and research security also share a lack of empirical effectiveness, where the literature argues for better implementation of regulations to achieve the desired results (Pol, 2018). Specifically, in terms of standard-setting, it has been pointed out that 'primary reliance is still placed on expertise of the FATF member delegations rather than research and objective analysis' (de Koker, 2022, pp. 265–267). Further, recommendations in both fields tend to focus on the identification and management of high-risk entities. This, along with the assumption that the regulators and regulated know how to appropriately apply these measures, is a consequence of the risk-based approach present in both frameworks. We need to consider how we can more effectively deal with research security regimes with this in mind, where any recommendations around research security should consider regulatory impact assessments as part of a more evidence-based standard-setting process (de Koker, 2022). These considerations also shed light on the facets of the AML/CTF regime that should be developed.

One shortfall that research security should also avoid is the inevitable clamour for piecemeal introductions based on sector need. Similar sentiments in the AML/CTF space led to Australia witnessing a significant delay—17 years—in the implementation of Tranche II regulations focused on incorporating DNFBPs within the framework (Parliament of Australia, 2024). Moreover, there is a need to ensure illicit actors cannot take advantage of national differences in the definition, scope and sanctioning of offences (which results in sub-optimal cooperation between concerned authorities: Tiwari et al., 2020). Consequently, this leads us to the question if these issues will arise in terms of research security regimes.

A final question arises on the financial implications for organisations based on current critiques of the AML/CTF regime. The sheer cost of administering the money laundering regime in the UK for example is approximately £28.7bn per year (LexisNexis, 2021). A large part of this spend is directed towards transaction monitoring technology and operations, a process that has noted efficiency issues (Pontes et al., 2022). This is one of the reasons why organisations may be reluctant to implement certain controls around research security: it costs money, and without a clear evidence-base for what the regime sets out to control, it risks having high transaction costs. Further, AML/CTF regimes have been met with reluctance and questioning from some industries where they currently do not have a great history of compliance; i.e., the casino sector. Known for being an industry commonly targeted by money launderers (Teichmann, 2018), the industry as a whole has pushed back on the adoption of AML/CTF regulations citing challenges around costs, conflict of interest with clients, lack of an evidence-base, and redundant data (Real Estate Institute of Australia, 2023). The university sector could

have a similar response, and we anticipate potential backlash from the academic community. Academic freedom is an essential component of universities (Butler, 2017) and one that is (rightly) fiercely protected by institutions and researchers. However, the freedom of academia in Australia is not absolute—the case of *Ridd* (2021) demonstrated that even the High Court considers the protection of legal rights of others as an appropriate ground for limiting that freedom. In the same vein, where unregulated research may cause outcomes contrary to the national interest, academic freedom may need to yield to the protection of Australian innovation and national security.

Part VII: conclusion

This paper has proposed a novel paradigm to tackle the threats to national security which can manifest at universities and threaten to subvert or divert technological innovations from their source. By critically examining some of the features of the AML/CTF regime in Australia and internationally, we have identified several tools that would be of significant relevance in identifying and mitigating those unique threats. However, the comparison has also identified certain flaws in the AML/CTF system that any research security programme should strive to avoid. Universities and governments will need to share risk in this space for the system to work. Emerging research is already showing that to continue international collaborations in contested or volatile geopolitical settings will require universities to:

> … develop guidelines that consider the increasingly multipolar research landscape amid geopolitical tensions. The research sector's inability to handle matters related to data security, multiple affiliations, or ethics dumping can mean that national political forces are likely to use additional compliance. (Shih et al., 2023, p. 15)

This paper has also achieved another purpose: to contribute to the vastly undertheorised notion of research security in academic literature. We have sought to co-design an approach that treats risk appropriately, and respect academic freedom without becoming entirely subservient to it. Our proposal is not a panacea—it will require individualisation amongst its stakeholders (similar to how financial institutions take bespoke methods to meet their AML/CTF obligations). Quite obviously, the involvement of foreign entities in sensitive or security-controlled research is quite the opposite intention of a research security scheme yet may be the actual outcome of a poorly implemented scheme and may count against it. But establishing a baseline of standards that is achievable and realistic for higher education is a key function of our proposal.

Similarly, engaging in this discourse promotes an uplift of security concepts across our higher education sector, and indeed in the AML/CTF regime. We do not compare universities and banks mildly—even the smallest tertiary education or financial institution is a complex and complicated entity, subject to a wide range of security threats. But by learning from the hard-won lessons of the AML/CTF framework, Australia's higher education research sector can have an easier time enacting its own controls for protecting research. Further research is clearly needed into areas of governance (other than presented here) which could serve as other levers for ensuring we do not lose our innovations and inventiveness to insidious or malicious security actors.

Notes

1. Finding that 'intellectual freedom is not qualified by a requirement to afford respect and courtesy in the manner of its exercise', but that academic freedom is qualified such that the exercise must be lawful and respect the legal rights of others: *Ridd v James Cook University* (2021) 274 CLR 495, at [64].
2. Proscribed by the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth) ('AML/CTF Rules'), section 8.1.3.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Brendan Walker-Munro http://orcid.org/0000-0001-5484-1145
Jamie Ferrill http://orcid.org/0000-0003-4238-8894
Milind Tiwari http://orcid.org/0000-0002-5948-1828

References

Alberto, G. S. (2016). Spain: Financial ownership file and money laundering prevention. *Journal of Money Laundering Control*, *19*(3), 238. https://doi.org/10.1108/JMLC-10-2014-0030

Alexander, K. (2007). The international anti-money laundering regime: The role of the Financial Action Task Force. *Journal of Money Laundering Control*, *4*(3), 231–248. https://doi.org/10.1108/eb027276

Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of applying machine learning for watch-list filtering in anti-money laundering. *IEEE Access*, *9*, 18481. https://doi.org/10.1109/ACCESS.2021.3052313

Angell, M. (2000). Is academic medicine for sale? *New England Journal of Medicine*, *342*(20), 1516–1518. https://doi.org/10.1056/NEJM200005183422009

APGML. (2024). *About APG*. https://apgml.org/about-us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162

Aurasu, A., & Rahman, A. A. (2018). Forfeiture of criminal proceeds under anti-money laundering laws: A comparative analysis between Malaysia and United Kingdom (UK). *Journal of Money Laundering Control*, *21*(1), 104–111. https://doi.org/10.1108/JMLC-04-2017-0016

AUSTRAC. (2024a). *Your obligations*. https://www.austrac.gov.au/business/new-to-austrac/your-obligations

AUSTRAC. (2024b). *AML/CTF Programs*. https://www.austrac.gov.au/business/core-guidance/amlctf-programs

Ayling, J., Grabosky, P., & Shearing, C. (2006). Harnessing resources for networked policing. In J. Fleming & J. Wood (Eds.), *Fighting crime together: The challenge of policing networks* (pp. 60–86). University of New South Wales Press.

Babina, T., He, A. X., Howell, S. T., Perlman, E. R., & Staudt, J. (2023). Cutting the innovation engine: How federal funding shocks affect university patenting, entrepreneurship, and publications. *The Quarterly Journal of Economics*, *138*(2), 895–954. https://doi.org/10.1093/qje/qjac046

Bamford, J. (2023, November 17). *Israel's war on American student activists*. https://www.thenation.com/article/world/israel-spying-american-student-activists/

Basel Committee on Banking Supervision. (2001). *Customer due diligence for banks report*.

Bernstein, L., Sun, L. H., & Rein, L. (2019, April 3). *NIH police yank Iranian graduate student from lab as agency clamps down on security*. https://www.washingtonpost.com/national/health-

science/nih-police-yank-iranian-graduate-student-from-lab-as-agency-clamps-down-on-security/2019/04/03/79f98bca-555a-11e9-8ef3-fbd41a2ce4d5_story.html
Burakovsky, A. (2022, 1 April). *The war in Ukraine ruins Russia's academic ties with the West*. https://theconversation.com/the-war-in-ukraine-ruins-russias-academic-ties-with-the-west-180006
Burgess, M. (2023). *Director-general's annual threat assessment*. https://www.asio.gov.au/director-generals-annual-threat-assessment-2023
Butler, J. (2017). Academic freedom and the critical task of the university. *Globalizations*, *14*(6), 857–861. https://doi.org/10.1080/14747731.2017.1325168
Canestri, D. (2019). Politically exposed entities: How to tailor PEP requirements to PEP owned legal entities. *Journal of Money Laundering Control*, *22*(2), 359–372. https://doi.org/10.1108/JMLC-06-2018-0042
Cassella, S. D. (2004). Terrorism and the financial sector: Are the right prosecutorial tools being used? *Journal of Money Laundering Control*, *7*(3), 281–285. https://doi.org/10.1108/13685200410809995
Chadderton, P., & Norton, S. (2019). *Public-private partnerships to disrupt financial crime: An exploratory study of Australia's FINTEL alliance*. Swift Institute Working Paper No. 2017-003.
Chaikin, D. (2009). How effective are suspicious transaction reporting systems? *Journal of Money Laundering Control*, *12*(3), 238–253. https://doi.org/10.1108/13685200910973628
Chaikin, D. (2018). A critical analysis of the effectiveness of anti-money laundering measures with reference to Australia. In C. King, C. Walker, & J. Gurulé (Eds.), *The Palgrave handbook of criminal and terrorism financing law* (pp. 293–316). Springer.
Cohen, A., & van der Steege, M. (1982). An historical overview of the state and higher education in the Netherlands. *European Journal of Education*, *17*(3), 271–274. https://doi.org/10.2307/1502985
Conley-Tyler, M., & Law, S. F. (2020, 27 November). *Australia's universities need to be free to engage globally*. https://pursuit.unimelb.edu.au/articles/australia-s-universities-need-to-be-free-to-engage-globally
Cosenza, I., & Connors, K. (2004). Protection and use of classified information in National Security cases. *Journal of the Australian Institute of Professional Intelligence Officers*, *13*(2), 5–16.
Council of the European Union. (2009). *Regulation No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*. https://eur-lex.europa.eu/eli/reg/2009/428/oj/eng
Crick, J. M., Friske, W., & Morgan, T. A. (2024). The relationship between coopetition strategies and company performance under different levels of competitive intensity, market dynamism, and technological turbulence. *Industrial Marketing Management*, *118*, 56–77. https://doi.org/10.1016/j.indmarman.2024.02.005
Dalla Pellegrina, L., & Masciandaro, D. (2009). The risk-based approach in the new European anti-money laundering legislation: A law and economics view. *Review of Law & Economics*, *5*(2), 931–952. https://doi.org/10.2202/1555-5879.1422
Daniels, M., & Krige, J. (2022). *Knowledge regulation and national security in postwar America*. University of Chicago Press.
de Koker, L. (2022). Editorial: Regulatory impact assessment: Towards a better approach for the FATF. *Journal of Money Laundering Control*, *25*(2), 265–267. https://doi.org/10.1108/JMLC-05-2022-149
de Koker, L. (2024). Editorial: FATF greylisting: Time to revisit the approach. *Journal of Money Laundering Control*, *27*(4), 621–624. https://doi.org/10.1108/JMLC-07-2024-206
de Koker, L., Howell, J., & Morris, N. (2023). Economic consequences of greylisting by the Financial Action Task Force. *Risks*, *11*(5), 81–113. https://doi.org/10.3390/risks11050081
Dudink, Y., Taminiau, Y., & Veenswijk, M. (2024). The dark side of public-private partnerships: Enforced hybridity and power dynamics in fighting financial crime. *Public Policy and Administration*, *39*(3), 497–518. https://doi.org/10.1177/09520767231191821

Enserink, M. (2015, 16 July). *Dutch appeals court dodges decision on hotly debated H5N1 papers*. https://www.science.org/content/article/dutch-appeals-court-dodges-decision-hotly-debated-h5n1-papers

Evans, S. A. W., & Valdivia, W. D. (2012). Export controls and the tensions between academic freedom and national security. *Minerva*, *50*(2), 169–190. https://doi.org/10.1007/s11024-012-9196-4

FATF. (2024). *History of the FATF*. https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html

French, R. (2019). *Report of the independent review of freedom of speech in Australian higher education providers*. Commonwealth Government Printer.

Goldbarsht, D. (2023). Adapting confiscation and anti-money laundering laws to the digital economy: Exploring the Australian interplay between proceeds and technology. *Journal of Money Laundering Control*, *27*(3), 472–488. https://doi.org/10.1108/JMLC-09-2023-0142

Goldbarsht, D., & Benson, K. (2024). From later to sooner: Exploring compliance with the global regime of anti-money laundering and counter-terrorist financing in the legal profession. *Journal of Financial Crime*, *31*(4), 472–488. https://doi.org/10.1108/JFC-08-2023-0201

Golden, D. (2018). *Spy schools: How the CIA, FBI, and foreign intelligence secretly exploit America's universities*. Picador.

Government of Canada. (2023). *Why safeguard your research?* https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/why-safeguard-your-research

Government of Canada. (2024a). *Policy on sensitive technology research and affiliations of concern*. https://ised-isde.canada.ca/site/science/sites/default/files/documents/2024-01/1154-policy-strac-en-final-09Jan2024.pdf

Government of Canada. (2024b). *Sensitive technology research areas*. https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1081-sensitive-technology-research-areas-09Jan2024.pdf

Government of Canada. (2024c). *Named research organizations*. https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1082-named-research-organizations-list-09Jan2024.pdf

Government of the Netherlands. (2023). *Contact point for knowledge*. https://english.loketkennisveiligheid.nl/

Grabosky, P. (2013). Beyond responsive regulation: The expanding role of non-state actors in the regulatory process. *Regulation & Governance*, *7*(1), 114–123. https://doi.org/10.1111/j.1748-5991.2012.01147.x

Greene, A. (2022, 10 February). *Intelligence officials identify Russian efforts to interfere in Australian politic*. https://www.abc.net.au/news/2022-02-10/russia-foreign-interference-australian-election/100819910

Group of Eight. (2021). *Measures to safeguard Australia's sensitive research*. https://go8.edu.au/wp-content/uploads/2021/03/Go8-Measures-to-Safeguard-Australias-Research.pdf

Group of Eight. (2022). Essential decisions for national success: reducing the regulatory overload on our universities. https://www.go8.edu.au/wp-content/uploads/2022/04/Go8-Reducing-the-regulatory-overload.pdf

Gup, B. E., & Beekarry, N. (2009). Limited liability companies (LLCs) and financial crimes. *Journal of Money Laundering Control*, *12*(1), 7–18. https://doi.org/10.1108/13685200910922615

Hare, J. (2023, 23 July). *Unis are bastions of conformity, not radical thinking: academic*. https://www.afr.com/work-and-careers/education/unis-are-bastions-of-conformity-not-radical-thinking-academic-20230720-p5dpud

Hartman, G. (2010). Australian university research commercialisation: Perceptions of technology transfer specialists and science and technology academics. *Journal of Higher Education Policy and Management*, *32*(1), 69–71. https://doi.org/10.1080/13600800903440568

Herlin-Karnell, E. (2017). The robustness of EU financial crimes legislation: A critical review of the EU and UK anti-fraud and money laundering scheme. *European Business Law Review*, *28*(4), 427–446. https://doi.org/10.54648/EULR2017023

ICIJ. (2024a). *The Panama Papers*. https://www.icij.org/investigations/panama-papers/

ICIJ. (2024b). *The Paradise Papers*. https://www.icij.org/investigations/paradise-papers/

ICIJ. (2024c). *The Pandora Papers*. https://www.icij.org/investigations/pandora-papers/

Jakobi, A. P. (2018). Governing illicit finance in transnational security spaces: The FATF and anti-money laundering. *Crime, Law and Social Change*, *69*(2), 173–190. https://doi.org/10.1007/s10611-017-9750-y

James, M. (2012). Growing confidence in educational research: Threats and opportunities. *British Educational Research Journal*, *38*(2), 181–201. https://doi.org/10.1080/01411926.2011.650681

Karran, T., & Mallinson, L. (2017). *Academic freedom in the U.K.: Legal and normative protection in a comparative context*. University and College Union.

Kerr, C. (1995). *The uses of the university*. Harvard University Press.

Kerr, P. K., & Casey, C. A. (2021). *The U.S. Export Control System and the Export Control Reform Act of 2018*. https://crsreports.congress.gov/product/pdf/R/R46814

King, C., & Walker, C. (2015). Counter terrorism financing: Redundant fragmentation? *New Journal of European Criminal Law*, *6*(3), 372–395. https://doi.org/10.1177/203228441500600308

Kiu, C. L., & Leung, F. S. (2023). A simulation game for anti-money laundering (AML) using unity. *Proceedings of the European Conference on Games-based Learning*, *17*(1), 117–126. https://doi.org/10.34190/ecgbl.17.1.1512

KNAW. (2023, 10 October). Royal Netherlands Academy of Arts and Sciences (KNAW) warns against proposed Knowledge Security Act. https://www.knaw.nl/en/news/royal-netherlands-academy-arts-and-sciences-knaw-warns-against-proposed-knowledge-security-act

Langdale, J. (2023). Money laundering in Australian casinos. *Journal of Money Laundering Control*, *26*(7), 99–109. https://doi.org/10.1108/JMLC-09-2022-0136

Legal and Constitutional Affairs References Committee. (2022, March). *The adequacy and efficacy of Australia's anti-money laundering and counterterrorism financing (AML/CTF) regime*. https://apo.org.au/sites/default/files/resource-files/2022-03/apo-nid317204.pdf

Lester, R., Tsai, L., Berger, S., Fisher, P., Fravel, M. T., Goldston, D., Huang, Y., & Rus, D. (2023). Managing United States-China university relations and risks. *Science*, *380*(6642), 246–248. https://doi.org/10.1126/science.adg5619

Levi, M., Reuter, P., & Halliday, T. (2018). Can the AML system be evaluated without better data? *Crime, Law and Social Change*, *69*(2), 307–328. https://doi.org/10.1007/s10611-017-9757-4

Lewis, J. A. (2017, 15 August). *Put China's intellectual property theft in a larger context*. https://www.csis.org/analysis/put-chinas-intellectual-property-theft-larger-context

LexisNexis. (2021). *Cutting the costs of AML compliance*. https://solutions.risk.lexisnexis.co.uk/cutting-the-costs-of-aml-compliance

Lynch, N. (2024, 1 March). *Australia creates world-first intelligence hub to fight financial crime*. https://www.linkedin.com/pulse/australia-creates-world-first-intelligence-hub-fight-financial-lynch/

Malakoff, D. (1999). Spy inquiry is taking toll on non-U.S. researchers. *American Association for the Advancement of Science*, *284*(5416), 882. https://doi.org/10.1126/science.284.5416.882

Mallapaty, S. (2023). China is mobilizing science to spur development — And self-reliance. *Nature*, *615*(7953), 570. https://doi.org/10.1038/d41586-023-00744-4

Manning, M., Wong, G. T. W., & Jevtovic, N. (2021). Investigating the relationships between FATF recommendation compliance, regulatory affiliations and the Basel Anti-Money Laundering Index. *Security Journal*, *34*(3), 566–588. https://doi.org/10.1057/s41284-020-00249-z

Maxwell, N. (2019). Expanding the capability of financial information-sharing partnerships. https://www.future-fis.com/uploads/3/7/9/4/3794525/pr%C3%A9cis_of_ffis_paper_-_expanding_the_role_of_fisps_-_march_2020.pdf

Maxwell, N., & Artingstall, D. (2017). The role of financial information-sharing partnerships in the disruption of crime. https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_report_-_oct_2017.pdf

McFadden, C., Nadi, A., & McGee, C. (2018, 24 July). Education or espionage? A Chinese student takes his homework home to China. https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881

Mervis, J. (2019, 26 April). U.S. universities reassess collaborations with foreign scientists in wake of NIH letters. https://www.science.org/content/article/us-universities-reassess-collaborations-foreign-scientists-wake-nih-letters

Miller, D., & Massoumi, N. (2015, 16 June). University research on terrorism may never be free from interference. https://www.theguardian.com/higher-education-network/2015/jun/15/university-research-terrorism-without-state-government-rightwing-interference

Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, *59*(6), 411–423. https://doi.org/10.1007/s12599-017-0504-2

Mugarura, N. (2014). Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm. *Journal of Money Laundering Control*, *17*(1), 76–95. https://doi.org/10.1108/JMLC-07-2013-0024

Naheem, M. A. (2020). The agency dilemma in anti-money laundering regulation. *Journal of Money Laundering Control*, *23*(1), 26–37. https://doi.org/10.1108/JMLC-01-2016-0007

Nance, M. T. (2018). Re-thinking FATF: an experimentalist interpretation of the Financial Action Task Force. *Crime, Law and Social Change*, *69*(2), 131–152. https://doi.org/10.1007/s10611-017-9748-5

National Research Council of the National Academies. (2009). *Beyond "Fortress America"*. National Academies Press.

Norton, S. (2017, 15 September). Lessons from the CBA money-laundering scandal. https://www.aspistrategist.org.au/lessons-cba-money-laundering-scandal/

Norton, S. (2018). Suspicion of money laundering reporting obligations: auditor compliance, or sceptical failure to engage? *Critical Perspectives on Accounting*, *50*, 56–66. https://doi.org/10.1016/j.cpa.2017.09.003

NPSA. (2023). *Trusted Research*. https://www.npsa.gov.uk/trusted-research

Parliament of Australia. (2024). Final Report of the Legal and Constitutional Affairs Legislation Committee on the Anti-Money Laundering And Counter Terrorism Financing Amendment Bill 2024. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Anti-MoneyLaundering47/Report

Patrone, D., Resnik, D., & Chin, L. (2012). Biosecurity and the review and publication of dual-use research of concern. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, *10*(3), 290–298. https://doi.org/10.1089/bsp.2012.0011

Pavlidis, G. (2023). The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards. *Journal of Economic Criminology*, *2*, 100040, 1–6. https://doi.org/10.1016/j.jeconc.2023.100040

Pisa, M. (2019). Does the Financial Action Task Force (FATF) help or hinder financial inclusion? A study of FATF mutual evaluation reports. https://www.cgdev.org/sites/default/files/does-financial-action-task-force-fatf-help-or-hinder-financial-inclusion-study-fatf.pdf

PJCIS. (2022). *Inquiry into national security risks affecting the Australian higher education and research sector*. Commonwealth Government Printer.

Pol, R. (2018). Anti-money laundering effectiveness: Assessing outcomes or ticking boxes? *Journal of Money Laundering Control*, *21*(2), 215–230. https://doi.org/10.1108/JMLC-07-2017-0029

Pontes, R., Lewis, N., McFarlane, P., & Craig, P. (2022). Anti-money laundering in the United Kingdom: New directions for a more effective regime. *Journal of Money Laundering Control*, *25*(2), 401–413. https://doi.org/10.1108/JMLC-04-2021-0041

Real Estate Institute of Australia. (2023). Modernising Australia's anti-money laundering and counter-terrorism financing regime. https://reia.com.au/wp-content/uploads/2023/07/AML_REIA-Submission-130723.pdf

Rechtschaffen, D. (2020, 11 November). How China's legal system enables intellectual property theft. https://thediplomat.com/2020/11/how-chinas-legal-system-enables-intellectual-property-theft/

Rijksoverheid [Government of the Netherlands]. (2020, 27 November). *Kamerbrief over maatregelen kennisveiligheid hoger onderwijs en wetenschap* [Letter to the House of Representatives on measures to secure knowledge in higher education and science]. https://www.rijksoverheid.nl/documenten/kamerstukken/2020/11/27/kennisveiligheid-hoger-onderwijs-en-wetenschap

Rijksoverheid [Government of the Netherlands]. (2023). *Loket Kennisveiligheid* [Contact point for knowledge security]. https://english.loketkennisveiligheid.nl/

Riondet, S. (2018). The value of public-private partnerships for financial intelligence. *Journal of Financial Compliance*, *2*(2), 148–154. https://doi.org/10.69554/YEAP9310

Ross, S., & Hannan, M. (2007). Australia's new anti-money laundering strategy. *Current Issues in Criminal Justice*, *19*(2), 135–150. https://doi.org/10.1080/10345329.2007.12036422

Sansonetti, R. (2000). The mutual evaluation process: A methodology of increasing importance at international level. *Journal of Financial Crime*, *7*(3), 218–226. https://doi.org/10.1108/eb025942

Saravalle, E. (2022). Recasting sanctions and anti-money laundering: From national security to unilateral financial regulation. *Columbia Business Law Review*, *1*, 550–620.

Sathye, M. (2008). Estimating the cost of compliance of AMLCTF for financial institutions in Australia. *Journal of Financial Crime*, *15*(4), 347–363. https://doi.org/10.1108/13590790810907191

Sathye, M., & Islam, J. (2011). Adopting a risk-based approach to AMLCTF compliance: The Australian case. *Journal of Financial Crime*, *18*(2), 169–182. https://doi.org/10.1108/13590791111127741

Schünemann, H., Al-Ansary, L., Forland, F., Kersten, S., Komulainen, J., Kopp, I., & Macbeth, F. (2015). Guidelines International Network: Principles for disclosure of interests and management of conflicts in guidelines. *Annals of Internal Medicine*, *163*(7), 548–553. https://doi.org/10.7326/M14-1885

Scott, B., & Webster, M. (2024). Anti-Money Laundering/Counter-Terrorism Financing Tranche 2 reform in Australia - An opportunity for intelligence to lead the way. *International Journal of Intelligence Issues*, *1*(1), 3–19.

Scott, P. F. (2023). "State threats", security, and democracy: The national security act 2023. *Legal Studies*, *1*, 1–17. https://doi.org/10.1017/lst.2023.39

Shih, T. (2024). Recalibrated responses needed to a global research landscape in flux. *Accounting Research*, *31*(2), 73–79.

Shih, T., Chubb, A., & Cooney-O'Donoghue, D. (2023). Scientific collaboration amid geopolitical tensions: A comparison of Sweden and Australia. *Higher Education*, *15*, 1339–1356. https://doi.org/10.1007/s10734-023-01066-0

Siddiqui, Z. (2023, 19 October). Five Eyes intelligence chiefs warn on China's 'theft' of intellectual property. https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/

Snetselaar, D. (2022). Dreams Lab: Assembling knowledge security in Sino-Dutch research collaborations. *European Security*, *32*(2), 233–251. https://doi.org/10.1080/09662839.2022.2127317

Stephenson, S. (2020). Dignity and the Australian constitution. *Sydney Law Review*, *42*(2), 369–394.

Strange, S. (1998). *Mad money when markets outgrow governments*. The University of MI Press.

Teichmann, F. M. T. (2018). Real estate money laundering in Austria, Germany, Liechtenstein and Switzerland. *Journal of Money Laundering Control*, *21*(3), 370–375. https://doi.org/10.1108/JMLC-09-2017-0043

Thomson, V. (2023, 21 February). *Opening statement to the Parliamentary Joint Committee on Intelligence and Security, Review of The Foreign Influence Transparency Scheme act 2018*. https://go8.edu.au/opening-statement-to-the-parliamentary-joint-committee-on-intelligence-and-security-review-of-the-foreign-influence-transparency-scheme-act-201-vicki-thomson

Tiwari, M., Ferrill, J., & Mehrotra, V. (2023). Using graph database platforms to fight money laundering: Advocating large scale adoption. *Journal of Money Laundering Control*, *26*(3), 474–487. https://doi.org/10.1108/JMLC-03-2022-0047

Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: The state of research in key areas. *Pacific Accounting Review*, *32*(2), 271–303. https://doi.org/10.1108/PAR-06-2019-0065

Tomoshige, H. (2022, 25 July). *The unintended impacts of the U.S. export control regime on U.S. innovation*. https://www.csis.org/blogs/perspectives-innovation/unintended-impacts-us-export-control-regime-us-innovation

Transparency International. (2019). *Who is behind the wheel? Fixing the global standards on company ownership*. https://www.transparency.org/en/publications/who-is-behind-the-wheel-fixing-the-global-standards-on-company-ownership

Trump, D. (2021, 14 January). *Presidential memorandum on United States government-supported research and development national security policy*. https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/
UKRI. (2024). Trusted research and innovation. https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/
Unger, B., Ferwerda, J., van Der Broek, M., & Deleanu, I. (2014). *The economic and legal effectiveness of the European Union's anti-money laundering policy*. Edward Elgar.
United Nations. (1966). *International Covenant on Civil and Political Rights.*
United Nations. (1988). *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. https://www.unodc.org/pdf/ convention_1988_en.pdf
Upton, B. (2023, 18 October). Dutch research security rules "virtually impossible to implement". https://www.timeshighereducation.com/news/dutch-research-security-rules-virtually-impossible-implement
Van der Sloot, B., & Kosta, E. (2019). Big brother watch and others v UK: Lessons from the latest Strasbourg ruling on bulk surveillance. *European Data Protection Law Review*, *5*(2), 252–265. https://doi.org/10.21552/edpl/2019/2/16
Van Duyne, P. C., Harvey, J. H., & Gelemerova, L. Y. (2018). *The critical handbook of money laundering: Policy, analysis and myths*. Palgrave McMillan.
Van Duyne, P. C., Harvey, J. H., & Gelemerova, L. Y. (2018). A 'risky' risk approach: proportionality in ML/TF regulation. In C. King, C. Walker, & J. Gurulé (Eds.), *The Palgrave handbook of criminal and terrorism financing law* (pp. 345–374). Springer.
VSNU. (2021). *Framework of knowledge security at Dutch universities*. https://vsnu.nl/files/documenten/Domeinen/Integrale%20veiligheid/VSNU%20Framework%20Knowledge%20Security%20Dutch%20Universities.pdf
Walker, S. (2020). *Review of the adoption of the model code on freedom of speech and academic freedom*. Commonwealth Government Printer.
Walker-Munro, B. (2021). A case for the use of cyber-systemics to combat financial crime in Australia. *Kybernetes*, *50*(11), 3082–3105. https://doi.org/10.1108/K-09-2020-0581
Walker-Munro, B. (2024a). Foreign interference and higher education research: AUKUS as a case study. *Journal of Higher Education Management*, *39*(1), 41–64.
Walker-Munro, B. (2024b). Politically exposed persons (PEP) screening: A solution to threats to research security? *Australian Business Law Review*, *52*(2), 75–95.
Wassink, J. (2023, 9 June). *A knowledge security law? Then screen everyone*. https://delta.tudelft.nl/en/article/knowledge-security-law-then-screen-everyone
Wilner, A., Beach-Vaive, S., Carbonneau, C., Hopkins, G., & Leblanc, F. (2022). Research at risk: Global challenges, international perspectives, and Canadian solutions. *International Journal: Canada's Journal of Global Policy Analysis*, *77*(1), 26–50.
Zavoli, I., & King, C. (2021). The challenges of implementing anti-money laundering regulation: An empirical analysis. *The Modern Law Review*, *84*(4), 740–771. https://doi.org/10.1111/1468-2230.12628

List of cases

Li v Canada (Citizenship and Immigration), 2023 FC 1753.
Ridd v James Cook University (2021) 274 CLR 495.
X established in Z v Minister for Foreign Trade and Development Cooperation. (2013, September 23). District Court of Noord-Holland. https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBNHO:2013:8527
X to Z v Minister for Foreign Trade and Development Cooperation. (2015, June 18). Amsterdam Court of Appeal. https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2015:2913&keyword = ECLI:NL:GHAMS:2015:2913