INNOVATION & RESEARCH CAUCUS

TRUSTED RESEARCH AND INNOVATION

How Knowledge Leakage Affects the Research & Innovation Ecosystem

IRC Report No: 024

REPORT PREPARED BY

Nicola Searle
Goldsmiths, University of London

Bernhard Ganglmair
University of Mannheim and ZEW Mannheim

Maurizio Borghi
University of Turin

Delivered with ESRC and Innovate UK

CONTENTS

Authors
The core members of the research team for this project were as follows:

- Nicola Searle – Goldsmiths, University of London
- Bernhard Ganglmair - University of Mannheim and ZEW Mannheim
- Maurizio Borghi – University of Turin

This document relates to IRC Project FFOpen002: Trusted Research & Innovation: An investigation of knowledge leakage.

Acknowledgements

This work was supported by Economic and Social Research Council (ESRC) grant ES/X010759/1 to the Innovation and Research Caucus (IRC). We are very grateful to the project sponsors at UK Research & Innovation (UKRI) for their input into this research. The interpretations and opinions within this report are those of the authors and may not reflect the policy positions of UKRI or its constituent councils.

The authors would like to thank the many people who contributed to the development of this report, including several unnamed policymakers and academics, Professor Stephen Roper and Sapna Marwaha, CEO and Founder of Formation Consultancy.

We would also like to acknowledge and appreciate the efforts of the IRC Project Administration Team involved in proofreading and formatting, for their meticulous attention to detail and support.

About the Innovation and Research Caucus

The Innovation and Research Caucus supports the use of robust evidence and insights in UKRI's strategies and investments, as well as undertaking a co-produced programme of research. Our members are leading academics from across the social sciences, other disciplines and sectors, who are engaged in different aspects of innovation and research systems. We connect academic experts, UKRI, IUK and the (ESRC), by providing research insights to inform policy and practice. Professor Tim Vorley and Professor Stephen Roper are Co-Directors. The IRC is funded by UKRI via the ESRC and IUK, grant number ES/X010759/1. The support of the funders is acknowledged. The views expressed in this piece are those of the authors and do not necessarily represent those of the funders.

Cite as: Searle, N., Ganglmair, B. & Borghi, M. 2025. *Trusted Research & Innovation: An investigation of knowledge leakage*. Oxford, UK: Innovation and Research Caucus

Executive Summary

Innovation drives economic growth and enhances social well-being. A robust Research & Innovation (R&I) ecosystem is essential for progress, economic resilience, and addressing complex challenges.

At the heart of this ecosystem, knowledge fuels innovation and further discovery. However, knowledge leakage (the loss of valuable information) can disrupt this cycle. This poses a challenge for what is known as Trusted Research & Innovation (TRI), a framework designed to strengthen research security, protect national interests, and build resilient research systems. Despite its significance to TR&I, knowledge leakage in this context is poorly understood.

This report investigates knowledge leakage. It begins with an overview of the TRI context, focusing on policymaking, and then reviews the literature on knowledge leakage and related concepts. An exploratory data analysis examines novel empirical data to better understand the extent of knowledge leakage and how it impacts economic areas of defence, economic and national security importance. The data analysis finds that industries deemed important for economic and national security (the UK's 'sensitive economic areas') have a 18% higher incidence of leakage than those that are not.

Context

Globally, interest in protections against knowledge leakage, and research security in general, is rapidly increasing. Countries throughout the world have enacted TRI policies. As innovation becomes more important for the economy and at the national level, innovation has joined the wider narrative of research security, economic security and ultimately national security.

Research security has long been an important policy and practice in the research & innovation ecosystem. In the UK, this policy and practice sits across funders, government departments, universities and sector collaboration and trade bodies. These organisations engage in a host of activities, including TRI and TRI-adjacent legislation and support via awareness and education. The EU has adopted recommendations to increase research security, and member states are devoting more resources to TRI policies and support. The US has long focused on knowledge leakage via espionage, with legislation steadily expanding since the mid-1990s. Not all countries are adopting legislative approaches, with some entities and countries encouraging more devolved approaches and a focus on research culture rather than law (e.g. the European Code of Conduct for Research Integrity and Denmark's approach).

Research

Research confirms the importance of knowledge flows, but also the downsides of knowledge leakage. The research is very clear on the benefits of knowledge flows to innovation and the economy, with much of these benefits coming from the movement of highly skilled workers and inter-organisational collaborations. There is also good support for the international migration of skilled works and international collaborations as vehicles for knowledge flows and innovation.

Knowledge leakage is generally negative for the firm losing the knowledge, although not exclusively so. Knowledge leakage of core knowledge may have a negative impact, but leaked knowledge that is not core may have no impact. Indeed, knowledge leakage may be beneficial in collaborations due to norms of reciprocity, as knowledge sharing between firms encourages more knowledge sharing. While there is limited research on the benefits to receiving leaked knowledge, it is generally considered beneficial for the firm.

Protecting against knowledge leakage is recognised as a challenge. Firms adopting protectionist policies and mechanisms harm knowledge flows and damage employee trust – neither of which is conducive to innovation. At the same time, uncontrolled knowledge leakage can damage a firm's innovativeness. However, the literature generally emphasises knowledge flows as an essential resource for innovation.

Data Analysis and Findings

To investigate the dynamics of knowledge leakage and its role in research security, we use data from research on knowledge leakage litigation and create a novel dataset of patents. Knowledge leakage is measured using trade secrets litigation data—694 EU cases from 2017 to 2022—capturing instances where firms took legal action over leaked trade secrets (Borghi et al., 2023). Firms use patents as a legal mechanism to protect against the copying of their innovations. Because industries and technologies vary in how likely they are to patent, knowledge leakage should influence patenting decisions differently across industries. To explore this, we examine knowledge leakage and patent behaviour, expecting greater reliance on patents in industries where leakage is perceived as a bigger threat— as patents provided a different mechanism for protection. We also consider whether knowledge leakage and patenting patterns differ in industries defined as being sensitive economic areas by UK security policies (i.e. the National Security and Investment (NSI) Act of 2021).

We find knowledge leakage is most prevalent, relative to industry size, in manufacturing and electricity, gas, steam and air conditioning supply. However, by technology it is most prevalent in chemistry. We find a positive correlation that firms in industries with high levels of knowledge leakage also patent more. This suggests our research framing that knowledge

leakage could cause firms to patent more is valid; however, our finding is correlation and not causation.

To place the analysis in the TRI context, we find the NSI economic sensitive areas are 18% more exposed to knowledge leakage than areas that are not sensitive. This is pronounced in Synthetic Biology, which has the highest prevalence of knowledge leakage. This stems from several factors, and we suspect Synthetic Biology, as a multi-disciplinary area working across different research units, has higher knowledge flows and therefore more opportunities for knowledge leakage. We also find sensitive economic areas patent four times as much as non-sensitive areas. Higher growth rates in patenting are observed in both technologies with high levels of knowledge leakage and in sensitive economic areas. However, these findings should be caveated by known differences in patenting rates across industries and technologies.

Implications

This report sets out the foundations for understanding how knowledge operates under a TRI lens by exploring the policy context, research, and empirical evidence on knowledge leakage. Policy responses to TRI-related risks are not straightforward, as they must balance national and economic security, protection against leakage, support for knowledge flows, and the need to sustain innovation. To date, approaches have centred on command-and-control measures (e.g. export controls), restricting knowledge flows (e.g. vetting collaborations, limiting licensing), support (e.g. awareness and compliance initiatives) and intellectual property protections. Our findings present the following implications, as three themes of actions to support TRI in the context of knowledge leakage:

Research

- Better understanding of knowledge leakage in sensitive economic areas could be valuable for developing more targeted strategies.
- Developing the evidence base on the impact of restrictions arising from TRI and TRI-adjacent policies on international collaborations and highly skilled labour could provide insights for policymaking.
- Exploring how IP management strategies can protect against knowledge leakage, and investigating how this varies by discipline, industry, or technology, could aid the development of practical approaches to knowledge leakage management.

Regulation

- Extending IP licensing restrictions may have unintended and counterproductive consequences.
- Exploring how policies can foster trust and TRI-positive cultures could inform the development of softer policies that provide effective complements to harder policies.

Refinement

- Conducting a cost-benefit analysis of TRI regulations on innovation could provide insights into their overall impact and inform future policy.
- Maintaining existing TRI support activities, and periodically evaluating them, could help ensure they continue to meet evolving needs.
- Aligning incentives between universities and their employees could support joint efforts to prevent knowledge leakage.
- Further reflection on how universities define undesirable knowledge leakage may clarify their protective strategies.

1. Introduction

Innovation is an important source of economic growth and improved social wellbeing. A healthy Research & Innovation (R&I) ecosystem, which consists of organisations, individuals and resources, enables innovation. This ecosystem drives progress, fosters the resilience of economies, helps solve complex problems, and creates new opportunities. Yet supporting innovation is a challenge. Navigating competing priorities within the R&I ecosystem, governments and firms face the delicate task of protecting existing innovations while encouraging new innovations.

A key resource for the R&I ecosystem is knowledge. Knowledge enables innovation and spurs the creation of further knowledge. However, loss of the exclusivity of that knowledge, where a third party gains access to that knowledge, can compromise innovation and knowledge creation. In the interests of brevity, we refer to this loss of exclusivity as the 'loss' of knowledge. Knowledge leakage is similar to, but distinct from, knowledge spillovers. While spillovers are generally viewed positively, as mutually beneficial and occurring more passively, knowledge leakage is typically considered negative. Leakage tends to be a more active phenomenon, where one party may benefit at the cost of another.

Supporting knowledge for R&I means managing competing priorities. On the one hand, it is important to protect against the loss of existing knowledge (knowledge leakage). On the other hand, it is important to encourage the movement of knowledge (knowledge flows) as they are a part of virtuous circle in which knowledge spurs innovation and knowledge creation. Paradoxically, knowledge leakage increases knowledge flows as leakage means knowledge is, for better or worse, flowing. Measures to protect against knowledge leakage and to encourage knowledge flows are not mutually beneficial. Protecting against knowledge leakage involves restricting knowledge flows, and encouraging knowledge flows increases the likelihood of knowledge leakage.

Knowledge flows, and leakage, are important but different at three levels of the R&I ecosystem – firm, domestic and international. At the most basic level, knowledge flows within a firm impact the innovativeness and research success of the firm. Knowledge leakage within a firm is possible, as firms may strategically choose to create internal silos[1] to manage knowledge flows and unwanted leakage between silos can undermine this choice. Knowledge flows within the domestic ecosystem are desirable as they contribute to the innovativeness of the domestic economy. Knowledge leakage within the domestic ecosystem - between domestic firms - may be undesirable for the firms but may benefit the domestic economy (i.e. leakage at the domestic level is not a zero-sum game.) Finally, international knowledge flows benefit innovation globally. However, international knowledge

[1] Siloing internal knowledge may be required for reasons of client confidentiality or other contractual/regulatory requirements; equally managing internal knowledge flows is important for managing external knowledge flows.

leakage – leakage between domestic ecosystems – is largely considered undesirable. While it may provide global benefits, the geopolitical nature of the 'unit' of a domestic ecosystem emphasises losses to domestic ecosystems. Indeed, much of the innovation and research policy focus of knowledge leakage addresses international knowledge leakage, i.e. leakage across political boundaries (borders).

Protection against knowledge leakage while fostering knowledge flows is a core part of what is called Trusted Research & Innovation (TRI). TRI is a research and innovation security policy agenda that seeks to promote research security, safeguard national interests and build resilient research ecosystems. Yet our current understanding of the extent of the role of knowledge leakage in research security remains limited and there is a lack of comprehensive analysis. To investigate these tensions, this exploratory report examines how organisations respond to knowledge leakage via a study of knowledge protection strategies in the context of knowledge leakage. It begins with an overview of the context of TRI, with a focus on policymaking, then develops a review of the literature addressing knowledge leakage and related terms before presenting the empirical research on knowledge leakage. The report concludes with a discussion of the implications of the research finding and how they might support TRI going forward.

2. Context

Policies protecting knowledge are fundamentally innovation policies. This section provides an overview of recent developments in innovation policies related to the loss of knowledge (knowledge leakage) in research environments, with a focus on public policy and research conducted in universities.

2.1 Addressing Challenges in Protecting UK Innovations in the Public Sector

A key area of interest for UK innovation policymakers and stakeholders is safeguarding intellectual property (IP) and sensitive technologies against threats – in particular protecting knowledge from the threat of knowledge leakage. To address these challenges, UK organisations such as UKRI (UK Research & Innovation)[2], universities and UUK (Universities UK, the trade body representing UK universities) have directed resources and policies to protect UK innovations from potential threats, including threats from collaborators, state-sponsored entities, and rival organisations. However, while protective measures are essential for bolstering research, economic and national security, they also may pose unintended consequences, as mechanisms restricting knowledge flows also impact knowledge flows in innovation.

These challenges are collectively known as Trusted Research and Innovation (TRI). TRI addresses the practice of conducting research transparently, and ethically. UKRI, which in 2023 identified TRI as an important risk for the UK (UKRI, 2023), describes TRI as:

> *'Trusted research' is a research and innovation sector term for protecting the UK's intellectual property, sensitive research, people and infrastructure from potential theft [knowledge leakage], manipulation and exploitation, including as a result of interference by hostile actors.*[3]

To assist universities and research organizations in managing these complexities, sector collaboration and trade bodies such as The Association of Research Managers and Administrators (ARMA), Universities UK, and the Higher Education Export Control Association (HEECA), offer guidance, training to identify and mitigate leakage risks, to support staff, and ensure compliance with related UK government security protocols (such as the Academic Technology Approval Scheme (ATAS)). In addition, the Research Collaboration Advice Team (RCAT) provides advice to research institutions on the national security risks linked to international research. The Alan Turing Institute, the UK's national institute for data science and AI, has argued for further support, including increased

[2] UKRI, the non-departmental public body responsible for supporting research and knowledge exchange at higher education institutions. It includes Innovate UK, the UK's innovation agency. UKRI is sponsored by the UK's Department of Science, Innovation and Technology (DSIT).
[3] (UKRI, 2024)

regulation of academic research and more formalised reporting and transparency (Hughes et al., 2025).

Compliance with research security policies is not costless. A 2023 ARMA report finds a conservative estimate that UK research organisations directly spend between £9.5M and £10.8M on staff and specialist tools for research security regulatory compliance and due diligence annually (Johnson et al., 2023). The report also finds this is likely to increase, with 77% of research organisations and 88% of funders/sector bodies expecting costs to rise. In addition to these direct costs, there are indirect costs such as research staff time, the cognitive load of dealing with increased regulatory complexity, and missed opportunities (as the report notes, compliance hinders organisational responsiveness.)

TRI and broader research security policies have been criticised for having adverse effects. Researchers criticising Australian policies describe a chilling effect on collaborations and how the constraints imposed by research security policies impact academic freedom (Chubb et al., 2023). Concerns have also been expressed about the use of TRI policies for targeting international researchers (Kim, 2018; Marwaha, 2024). Organisations and policymakers will have to navigate these challenges.

2.2 Economic and National Security Concerns: TRI-adjacent policies

A unique element of TRI as an innovation policy area is its relationship with economic and national security concerns. Broader geopolitical competition between countries and an increasing emphasis on knowledge-based economies mean economic security policy is now part of national security policies - consequently TRI, as an innovation and research security policy imbedded in economic security, ultimately falls under national security policies. This broadens the framing of knowledge leakage policies from being predominantly innovation policies, to a wider view of protecting knowledge from overseas threats. Additionally, through a national security lens, some technologies and industries are of particular concern.

The UK has increased policy activity related to knowledge leakage and is associating it explicitly with theft orchestrated by foreign actors. In 2023, the National Security Act strengthened penalties for international knowledge leakage. Awareness campaigns, led by organisations including the National Protective Security Authority (NPSA), emphasise the importance of vigilance among researchers across the public and private sector in safeguarding against knowledge leakage, highlighting potential impacts on research and researchers' reputations. MI5, the UK security service, has briefed UK universities on TRI threats arising from hostile state actors (Williams, 2024).

Organisations in the UK R&I ecosystem have focused on knowledge leakage in TRI as part of national security. ARMA has noted the "increasingly complex geopolitical environment" has shifted research organisations' responsibilities to protect against TRI (Marwaha, 2022). UUK has similarly discussed security, describing the problems stemming from attempts "by

overseas/hostile/external actors or those acting on their behalf to illegitimately acquire academic research and expertise" (Universities UK, 2020). UKRI annual reports similarly acknowledge these elements (e.g. 2023 Annual Report).

National security concerns focus on sensitive economic areas and research, as these areas may be strategically important in defence and economic security and subject to additional government TRI-related policies. The National Security and Investment (NSI) Act of 2021 identifies 17 economic areas, largely organised around technologies, that fall under additional security controls and restrictions. These technologies largely consist of those with potential defence applications, including dual-use technologies, such as Advanced Materials or AI, which can have both civilian and defence applications. For example, Digital Twinning, which has received significant public research funding, can fall under this category. Other key technologies focus more on economic security and infrastructure, such as Communications and Energy, which are crucial to safety and the social and economic functioning of the UK. Technologies related to cybersecurity may also raise concerns, particularly Cryptographic Authentication. However, TRI-related national security policies negatively impact innovation and research in sensitive areas as these policies impose both research costs to meet regulatory requirements and constraints more generally. Such policies also raise barriers to entry. With the increase in spending on military and defence expected across Europe in 2025, innovation in sensitive economic areas will take on more importance.

2.3 Global Context

Globally, international agreements and discussions also touch on TRI, demonstrating the importance of knowledge leakage in international relations and diplomacy. The G20 (Group of 20 major countries) leader agreements include references to the protection of IP, with the 2015 agreement explicitly mentioning protections against knowledge leakage, "we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information" ((G20 Leaders, 2015), p. 6). The North Atlantic Treaty Organisation (NATO) described knowledge security as a threat to the prosperity of its members (Snetselaar et al., 2022). Obligations to protect against knowledge leakage are found in the World Trade Organisation's (WTO) Trade Related Aspects of Intellectual Property agreement (1996), the United States-Mexico-Canada Agreement (2019), amongst others.[4]

The US has been prominent in raising research security as an issue, both broadly and within the context of university research. Significant legislative actions at the federal level (The Economic Espionage Act of 1996 and the Defend Trade Secret Act of 2016) have expanded

[4]The authors thank Professor Russell Buchan for highlighting these.

the punishments for intentional[5] knowledge leakage. The National Science Foundation (NSF), the US public research funding body, has an Office of the Chief of Research Security Strategy and Policy (OCRSSP) and in 2024 granted USD$50M to establish an academic centre for research security (the Safeguarding the Entire Community of the U.S. Research Ecosystem Center). The 2025 America First Investment Policy[6] focuses on expanding the ability of the Committee on Foreign Investment in the United States (CFIUS) to restrict foreign actors' access to US skills and sensitive technologies. The US has emphasised not only the threat from hostile actors, but also the increased success and competitiveness of overseas economies. Legislative actions include increasing the responsibilities of universities, through both National Security Presidential Memorandum (NSPM-33) and statutory instruments (e.g. the 2022 CHIPS and Science Act) (National Science Foundation, 2023).

Australia has similarly increased the responsibilities of universities to perform due diligence and increased disclosure requirements. In 2019, it established the University Foreign Interference Taskforce (UFIT). Subsequent Australian policies have increased government oversight and powers over international research collaborations. Sweden has adopted a more devolved approach, with responsibility for 'responsible internationalisation' sitting with funding bodies and universities (Chubb et al., 2023).

The European Commission adopted recommendations to enhance research security in 2024, with the goal of enhancing research security (Directorate General for Research and Innovation, 2024). The recommendations propose enhanced risk assessments, awareness and training and information sharing. In 2024, Germany's government funding agency (the German Research Foundation, DFG) began discussions on developing more formalised approaches to TRI within its R&I ecosystem (Gabel, 2024). A survey in Italy conducted by the Italian Ministry of University and Research found approximately 90% of research institutions and universities recognised a need for enhanced research security (Turone, 2024).

It is worth noting that not all organisations or countries frame TRI as largely a knowledge leakage problem. Emphasis may instead be given to the integrity or trustworthiness of research, of which knowledge leakage is a subset of integrity. For example, The European

[5] Intentional knowledge leakage is also known as the theft of trade secrets; unintentional knowledge leakage is instead largely accidental (e.g. accidentally leaving documents containing the knowledge in a public place.) Ritala et al., 2015 frame these as knowledge leakage by employees. We expand the definition of intentional knowledge leakage to include both employees (insiders) and third parties (outsiders); indeed, employees are the main source of intentional knowledge leakage and are often the conduit by which the knowledge reaches third parties.

[6] Trump, D. J. (2025, February 21). America First Investment Policy. The White House. https://www.whitehouse.gov/presidential-actions/2025/02/america-first-investment-policy/

Code of Conduct for Research Integrity, developed by All European Academies (ALLEA), focuses first on the trustworthiness of research and then considers mutual respect for IP.

The narrative surrounding TRI policies often focuses on external, overseas threats (international knowledge leakage orchestrated by foreign actors) and publicly funded research. However, the evidence indicates the vast majority of knowledge leakage comes from existing employees (Almeling et al., 2010, 2009). US data also indicates most cases of knowledge leakage are intended for domestic benefits and not overseas (on file with author Searle).

3. Review of the Literature

A dominant concern of TRI is the risks posed by knowledge leakage. The literature on knowledge leakage, its nature and impact, and how to prevent it is growing but relatively under-developed. This report focuses on innovation aspects of knowledge flows and knowledge leakage and therefore concentrates on the management and economics literature. These two literatures examine how firms innovate and generate knowledge, and how they protect their knowledge and innovations from leakage. While the focus is on firms, rather than universities or other public research entities, the findings should apply across the R&I ecosystem.

3.1 Knowledge Flows

Knowledge flows, which are the transfer and sharing of knowledge, information, and expertise within and between organizations, individuals, or systems, facilitate innovation and economic growth (Sorenson et al., 2006; Adler and Hashai, 2007; Singh and Agrawal, 2011; Roper and Hewitt-Dundas, 2015). A vast body of empirical evidence demonstrates that the movements of workers, particularly high skilled workers, is the dominant enabler of knowledge flows (e.g. (Breschi and Lissoni, 2009). Migrant inventors stimulate beneficial knowledge flows within hiring firms and between countries (Bahar et al., 2020; Oettl and Agrawal, 2008). Edler et al., (2011), similarly find the international mobility of scientists enables knowledge flows that are complementary to domestic technology transfer and increase academic productivity. Collaborations between organisations and the licensing of knowledge (i.e. the licensing of IP) also enable knowledge flows and innovation (Grindley and Teece, 1997). Research is very clear that knowledge flows, and the movement of workers that enables them, benefit innovation.

In the economics literature, knowledge flows are framed around the concept of disclosure, where a firm's choice to patent its innovations is an active choice to increase knowledge flows. In patenting, the firm makes knowledge about its innovation public thereby contributing to knowledge flows. Patents create a centralised repository of disclosed, innovative knowledge which facilitates knowledge flows via licensing (Hegde and Luo, 2017) and spurs further knowledge creation (Furman et al., 2021; Hegde et al., 2023). When industries are constrained by from patenting (e.g. due to regulations), knowledge flows lessen, and knowledge creation weakens (Gross, 2023).

3.2 Knowledge Leakage

While knowledge flows are beneficial for innovation as a whole, firms holding knowledge may have a different view. Knowledge leakage can be intentional or unintentional (Ritala et al., 2015). Knowledge leakage is undesirable for firms and negatively impacts the competitiveness of a firm (Frishammar et al., 2015). *Unintentional* knowledge loss can be accidental (e.g. leaving documents in a public space) or incidental (e.g. a researcher

oversharing at a conference), whereas *intentional* knowledge leakage[7] can be referred to as commercial, corporate or industrial espionage, the theft of trade secrets, or IP theft (Ritala et al., 2015). A subset of intentional knowledge leakage is that of state-sponsored or economic espionage, which refers to intentional knowledge leakage designed to benefit a foreign entity.

While knowledge leakage is generally framed as having a negative impact on firms, not all leakage has the same effect. The leakage of non-core knowledge may have no impact, but leakage of core knowledge can have severe negative impacts on the firm (Frishammar et al., 2015). However, the negative impacts of knowledge leakage may be overstated (Arias-Pérez et al., 2020). Knowledge leakage may in fact facilitate inbound knowledge flows due to norms of reciprocity (Inkpen et al., 2019), as knowledge sharing between firms is facilitated by expectations that knowledge flows will be bi-directional (Ganglmair et al., 2020; Ganglmair and Tarantino, 2014; Grinblatt and Keloharju, 2001; Hellmann and Perotti, 2011).

Firms on the receiving end of leaked knowledge may benefit. There is limited research investigating the benefits to recipients or the advantages of perpetrating knowledge leakage, instead research has focused on how firms seek the related concept of knowledge spillovers. Knowledge spillovers are unintended knowledge flows, typically in the context of collaborations, not explicitly associated with loss (Ferenhof, 2016) and where firms benefit from collaborators' knowledge (Alberti and Pizzurno, 2017). The limited research focusing on those receiving leaked knowledge, as opposed to spillovers, similarly finds benefits for the recipient. In a study on international intentional knowledge leakage (economic espionage), Glitz and Meyersson, 2020 find East German espionage of West German knowledge benefited East Germany by reducing the productivity gap between East and West Germany by 6.3 percentage points. However, this was not a costless increase in productivity as the stolen Western technologies crowded out Eastern innovation.

3.3 Protecting Against Knowledge Leakage

Protecting against leakage can be a double-edged sword, particularly as the majority of knowledge leakage, intentional and unintentional, comes from employees. Within firms, protections involve limiting access to and dictating how knowledge can be used, both of which may convey a lack of trust from the employer to employees (Hannah, 2005). This lack of trust may hinder innovation by discouraging employees from investing in employer-owned knowledge and undermine organisational culture (Martins and Terblanche, 2003).

[7] This report addresses intentional knowledge leakage, as it is better aligned with the focus on trust within the TRI agenda.

Discouraging the internal circulation of knowledge also limits employee's ability to combine knowledge and generate further knowledge. There are also wider consequences, as such restrictions can limit employee's rights to move between jobs (Aydinliyim, 2022), raise the cost of moving between jobs (Marx, 2011), reduce post-employment entrepreneurship (Pathak et al., 2013) and reduce incentives for employers to providing training to their employees (Wang, 2021).

More broadly, protecting against knowledge leakage inevitably involves reducing knowledge flows as the movement of knowledge is restricted. This is a mixed blessing, as uncontrolled knowledge leakage compromises a firm's ability to innovate (Ritala et al., 2015), but knowledge flows are essential for innovation and the generation of further knowledge. This is true at both the firm and economy level. Equally, such protections are not costless and it is often difficult for us to assess ex ante the efficient number of resources to invest in efforts to limit knowledge leakage (Anderson et al., 2013).

3.4 Illicit Technology Transfer

Along a similar vein, technology transfer research focuses on the movement of technologies and innovations themselves. The emphasis in the technology transfer literature is on codified knowledge related to technologies, rather than the broader idea of knowledge. As with knowledge flows, technology transfer provides benefits to firms, regions and economies by supporting innovation (Bozeman, 2000; Bozeman et al., 2015). Relevant to our focus on knowledge leakage are illicit technology transfer (Glitz and Meyersson, 2020) and coercive (forced) technology transfer policies (Prud'homme et al., 2018). Forced or illicit technology transfer policies (Andrenelli et al., 2019; Prud'homme et al., 2018) result in technology transfer without the explicit consent of the owner of the technology. For example, countries may require that joint ventures involving domestic and overseas entities must be accompanied by the sharing of technologies and IP, or that Foreign Direct Investment include a domestic partner with similar expectations of the transfer of technology (Andrenelli et al., 2019). A country may also be lax in enforcing laws protecting innovations from imitation (Prud'homme et al., 2018). State-sponsored espionage similarly promotes the acquisition of technologies owned by others. Yet research finds such policies are inefficient forms of technology transfer (Macdonald, 1993) and may come at the longer cost of domestic innovation as the country fails to develop its own innovation capabilities (Glitz and Meyersson, 2020).

3.5 Multidisciplinary Insights

Several other research areas look at knowledge leakage. Legal scholarship has much to offer in terms of putting knowledge in its wider context and in particular the role of IP regulations and cybersecurity policies (Shackelford, 2016). Dreyfuss and Lobel, (2016), detail the development of the American narrative equating the protection of knowledge with national security and argue this narrative ultimately undermines American inventiveness.

Similarly, Effron, (2016), frames the knowledge protection policy changes as being heavily influenced by corporate lobbyists, in which the lobbyists co-opt economic and national security narratives to advance their less dramatic goal of increased knowledge protections. This has also led to concerns about the targeting of Asian-Americans by the US government (Kim, 2018). Vats, (2020), similarly tracks the emergence of a racialised narrative where the persons effecting knowledge leakage are now the national enemy of the industrious white American innovator.

Other areas of humanities and social sciences provide insights. International relations scholars frame intentional knowledge leakage as a modern tool of warcraft (Shackelford et al., 2017). State-sponsored hacking targeting COVID research labs demonstrates an escalation of cyber economic espionage (Lallie et al., 2021). Sociology has investigated the relationship between employees, employers and regulations in the name of knowledge leakage. David and Halbert, (2015), note key global trends: a shift from knowledge protection away from targeting firms and towards prosecuting individuals, an increase in regulations accompanying a deregulation of labour, and the shift of major economies going from 'poachers' of knowledge to 'gamekeepers'. Criminology and psychology offer insights into the motivations of employees who intentionally leak knowledge (Cole and Ring, 2005; Sandberg, 2015; Wall, 2013).

The research confirms knowledge flows are important to innovation and that both knowledge leakage itself and protections against knowledge leakage can be detrimental to innovation. However, the literature on knowledge leakage is relatively underdeveloped, and research on intentional knowledge leakage is even more limited.

4. Analysis: Patents and Knowledge Leakage

TRI focuses on the innovation and research ecosystem, where knowledge leakage threatens innovation. In this section, we empirically examine their relationship. We are interested in understanding how innovative firms respond to knowledge leakage in the management of their innovation and their innovation protection strategies. For practical and methodological reasons, our analysis focuses on innovation, as the application of knowledge, rather than the broader concept of knowledge itself. We conduct an analysis of firm patenting behaviours, where patents represent an innovation protection strategy, to understand how firms protect their innovations in environments with knowledge leakage.

4.1 Overview of Patents and Trade Secrets

There are two contrasting approaches that allow innovative firms to protect their innovations against knowledge leakage: patents and secrets. Patents are a formal legal instrument innovative firms may use to protect their innovations. In contrast to knowledge kept secret within the firm, a patent protecting an innovation is a public document. The knowledge in the patent is consequently publicly *disclosed*. Patents remove the possibility of knowledge leakage because of this choice to disclose the knowledge (i.e. what is public cannot be further 'leaked). Patents are therefore methodologically useful as they serve as proxies for innovative firms' R&D output and a measure of the degree of *controlled* disclosure of knowledge. In contrast, the firm may choose not to disclose the knowledge and keep it secret. However, such information can suffer from knowledge leakage. In this framing, knowledge leakage cases represent *uncontrolled* (and unwanted) disclosure and are expected to affect firms' innovation and disclosure decisions. The core difference between the two involves the firm's choice of disclosure. Patents require public disclosure of the knowledge, whereas secrets involve no disclosure (secrecy) of the knowledge.

Placing this discussion on disclosure into a legal framing, patents are property rights granted to innovators that enable them to prevent others from using their innovations for a specific amount of time (usually 20 years). To obtain a patent, firms submit detailed knowledge about the innovation that is published. True knowledge leakage cannot occur as the knowledge contained in the patent is public. In contrast, firms may opt to use trade secrets. Trade secrets are also property rights granted to innovators and enable them to protect against knowledge leakage. The legal status of trade secrets can last indefinitely if the knowledge remains secret. Knowledge leakage can occur with trade secrets as the firm can lose the knowledge via the loss of secrecy.

A substantial literature addresses the choice between innovative firm's choice of disclosure (patents) or not (trade secrets[8]). The use of disclosure via patenting varies by industry and technology. Pharmaceutical and chemical industries use patents more intensely and services less so (Chabchoub and Niosi, 2005). More innovative industries may also be more likely to use patents (Brouwer and Kleinknecht, 1999). The level or threat of knowledge leakage of knowledge leakage in an industry also pushes firms to rely more heavily on patents as their means of protection over secrets (Kang and Lee, 2022).

4.2 Research Agenda and Methodology

As industries and technologies have different propensities to patent, knowledge leakage should affect patenting in varying degrees across industries, including across the NSI Act's economic areas. To investigate this, we look at instances of knowledge leakage by industry and the impact on firms' decision to disclose knowledge via patenting.

We would expect to see firms patent relatively more when they perceive knowledge leakage to be more of a threat. Patents provide higher protection against knowledge leakage, as the knowledge is already disclosed and cannot be leaked. As we are also interested in the TRI aspects of the data, we additionally consider whether patent behaviour is different in industries where there is more focus on TRI.

To operationalise our areas of interest, we construct several variables. We measure instances of knowledge leakage (*KL*) by trade secrets litigation cases, in which one firm takes another firm to court over knowledge leakage in the form of a trade secret dispute (Borghi et al., 2023). This includes data on 694 trade secrets cases in the EU decided between 2017 and 2022; further details on the data collection process can be found in (Borghi et al., 2023).

To measure knowledge leakage by industry (*KLind*), we match the plaintiff firms in the TS litigation data to Orbis, from where we also get firm-level industry code, which we then aggregate to the 2-digit Statistical Classification of Economic Activities in the European Community (NACE) level for simplicity. This gives us the count of cases by industry and country. It is difficult to measure to what degree these cases are international instances, e.g. economic espionage. Using the postal addresses of the parties involved, 83% are domestic cases of knowledge leakage[9] and 12% are international cases of leakage[10], with the remaining cases unidentified. This is likely an underestimate of the number of international cases, as companies working across

[8] To note we focus on trade secrets rather than secrecy more generally as our data is exclusively trade secrets.
[9] Both parties are located in the jurisdiction of the case.
[10] At least one party is located outside the jurisdiction of the case.

borders will have offices in more than one jurisdiction and, regardless of the location of the leakage, the entity in the same jurisdiction of the case will be targeted.

The sample is fairly balanced in terms of firm size. On the side of the plaintiff (the party who has suffered knowledge leakage), there are 78 micro enterprises, 186 SME, 68 large corporation and 8 miscellaneous; however, we do not have information on 341 cases. On the defendant side, 236 (roughly 1/3) cases are against individuals and not firms. This is not uncommon, as individuals are typically former employees (193 of the cases) who may have planned to take the knowledge to a new employer or set up a new business but are sued before this actually happens (hence no firm to sue.) Of the cases involving organisations, 82 are micro enterprises, 122 SME, 29 large corporation and 26 miscellaneous; however, we do not have information on 188 cases. Overall, this suggests the sample does not suffer from a large-firm bias.

To account for differences in industry sizes, we scale the number of litigation cases by the total number of firms in the industry by country. This allows for a measure of what we call '*knowledge leakage exposure*' by industry, where we have a measurement of knowledge leakage in an industry. Higher values of knowledge leakage exposure indicate industries where knowledge leakage is relatively more common.

To understand disclosure behaviour, we take a series of steps involving technology identification, patent classes, sensitive economic areas and UK patenting. The first two steps are interim steps which allow us to calculate how industries vary their disclosure (patenting behaviour) based on knowledge leakage and TRI. In step one, we identify the patent classes, and subclasses, which are the classification of patents by technology area according to the Cooperative Patent Classification (CPC) system, in the industries affected by knowledge leakage. Using the NACE 2-digit codes of the industries in the knowledge leakage data, we convert these to the patent classes using the Lybbert-Zolas concordance table.[11] This allows us to calculate technology knowledge exposure by patent class, meaning we can connect disclosure behaviour by technology to knowledge leakage (*knowledge leakage by technology, KLpat*).

As we are interested in TRI aspects of knowledge leakage and disclosure, our second step is to pay particular attention to industries identified by the government as being important to national and economic security. We focus on the UK's 17 sensitive economic areas defined by the NSI Act of 2021, as described in the Introduction of this report) and their patenting behaviour. To do this, we develop a new concordance table

[11] The Lybbert-Zolas (Lybbert and Zolas, 2014) concordance table is a standard tool in patent analysis which matches industries to patent classes.

(see Table 8 in Appendix A: Concordance Table) based on the sensitive economic areas[12].

To develop our concordance table, we adopted three separate approaches which we then combined into a single table. We begin by feeding descriptions of sensitive economic areas into ChatGPT to extract the technology-relevant parts of the text. For the first approach, we then process those parts using the EPO's CPC classification tool[13]. For the second approach, focusing more on specific queries, we use Llama 3.3 to answer questions like, “what is synthetic biology, and which are the CPC patent classes used in this field?". For the third approach, we manually consult the CPC subclasses and main group descriptions identified in the first two approaches to understand what is covered and what is not. As part of this final approach, we also look to existing concordance tables on robotics, defence and military (Kim and Cho, 2022; Montobbio et al., 2022). Finally, using our subject matter expertise, we combine and refine the results from the three approaches. For additional quality control, we consulted patent experts and confirmed the match between the economic area and the patent class. This allows us to develop an indicator for disclosure in sensitive economic areas versus disclosure in economic areas not included in the list of 17.

Finally, we collect information on all UK patent applications at the UK Intellectual Property Office (UK IPO) including the count of patent applications in each patent class (based on the Cooperative Patent Classification (CPC) system) and the year the patent application was filed. Combining this with our technology exposure by patent class enables us to create *PatentTKind* which is a measure of the number of patents applications, by year, weighted by the knowledge leakage exposure of that year. This enables us to measure how industries change (or do not change) their disclosure behaviour following knowledge leakage exposure, by year. Finally, using our sensitive economic areas analysis, we can further divide these data into sensitive and non-sensitive technology area in the variable *PatentTKindTRI,* to enable us to understand whether this disclosure behaviour varies by sensitive and non-sensitive areas.

A summary of our final variables can be found in Table 1.

[12] We exclude two sensitive areas as they are not associated with technologies but the role of the firm. These are area 7 (Critical Suppliers of Government) and area 15 (Suppliers to the Emergency Services).
[13]https://epn.epo.org/cpc-text-categoriser

Table 1: Variables and Operationalisation

Variable of interest	Operationalisation label	Description of operationalisation
Knowledge leakage	Knowledge Leakage (*KL*)	Trade secrets litigation cases
Knowledge leakage exposure by industry	Knowledge Leakage by Industry (*KLind*)	Trade secrets litigation cases by industry, weighted by industry size
Knowledge leakage exposure by CPC patent class (technology)	Knowledge Leakage by Technology (*KLpat*)	Trade secret litigation cases by technology, as per CPC patent class
Decision to disclose knowledge in industries with higher knowledge leakage	Patenting by Industry and Knowledge Leakage (*PatentKLind*)	Number of patents in an industry, as measured by technologies and weighted by knowledge leakage exposure
Decision to disclose knowledge in industries with higher TRI concerns	Patenting by Industry and Knowledge Leakage and TRI (*PatentKLinTRI*)	Number of patents in an industry, as measured by technologies, weighted by knowledge leakage exposure and being in a sensitive economic area. N.B. This value is zero if the technology is not part of a sensitive economic area.

4.3 Exploratory Data Analysis

In this section, we provide an overview of our exploratory analysis. This enables us to have a snapshot of knowledge leakage and disclosure decisions as they stand. To start, we look at knowledge leakage exposure by industry (*KLind*), as presented in Figure 1. Two industries stand out as being particularly exposed to knowledge leakage – Manufacturing (NACE code C) and Electricity, gas, steam and air conditioning supply (NACE Code D). This figure is weighted by the size of the industry. Manufacturing has been found by several authors to be relatively vulnerable to knowledge leakage compared to other industries (Searle, 2021; Tan et al., 2016).

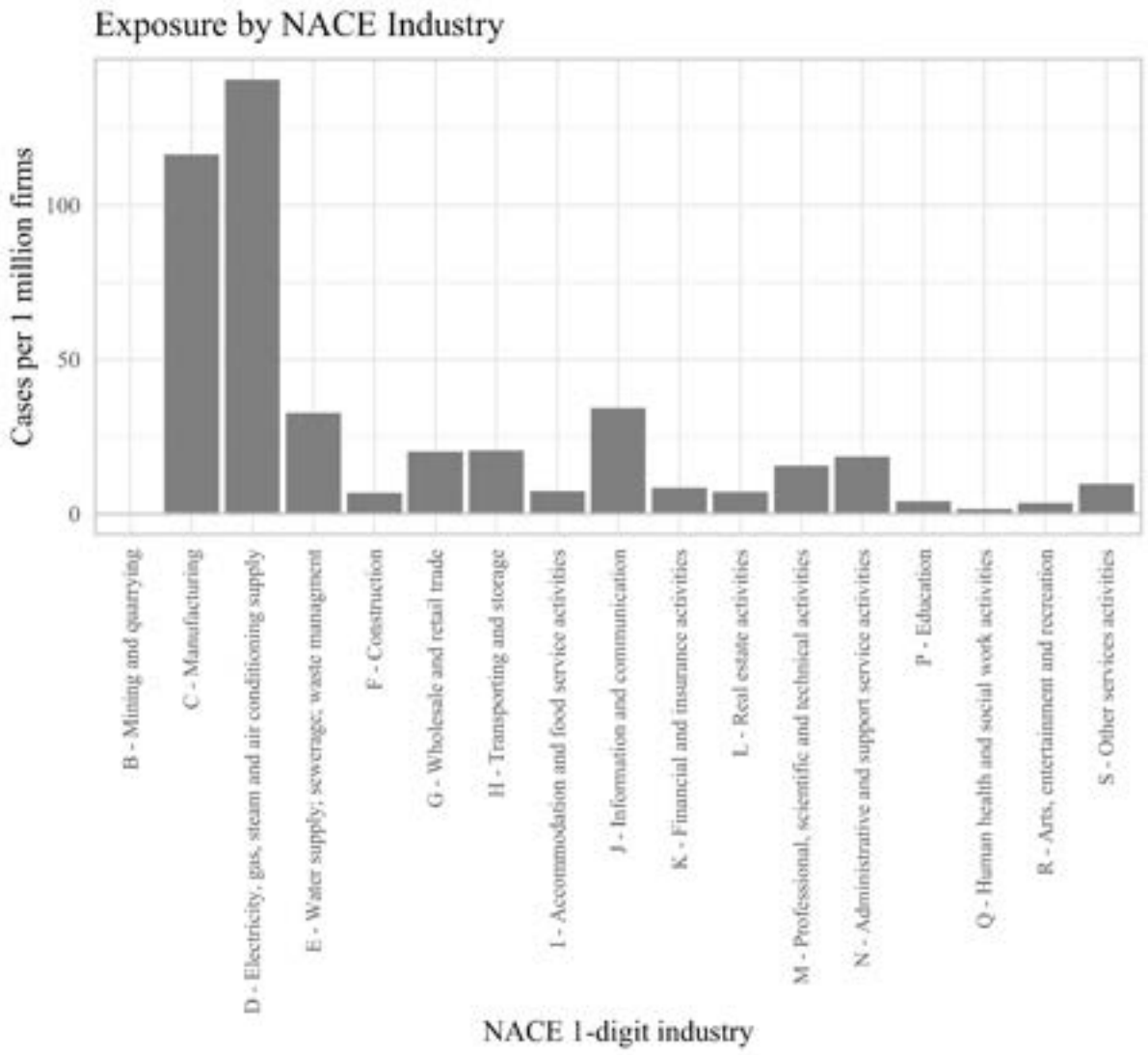

Figure 1: Knowledge Leakage by Industry

Second, we look at knowledge leakage by technology as classified by patent class (*KLpat*) as in Figure 2. The top technologies by knowledge leakage exposure are, in descending order: Chemistry (C0/C1), Health and Amusement (A6), Shaping (B2/B3), Engines or Pumps (F0), Combinatorial Technology (C4) and Engineering in General (F1).

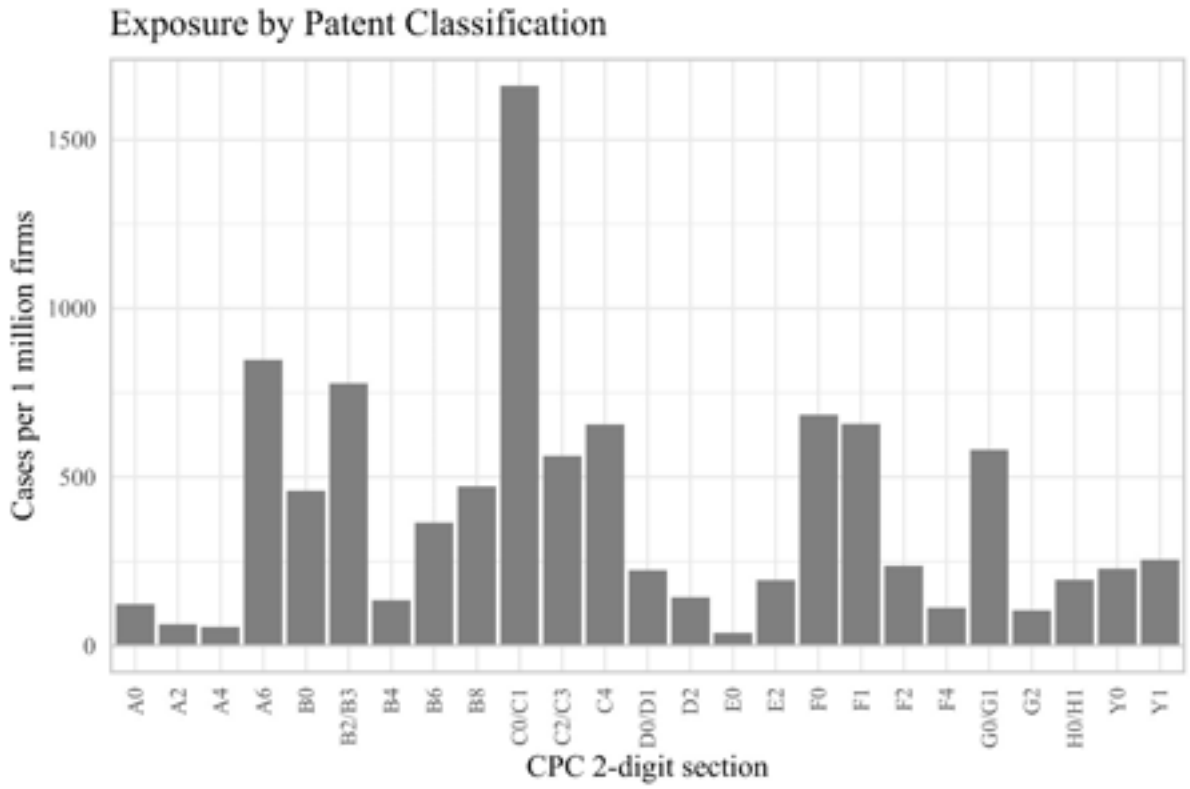

Figure 2: Knowledge Leakage by Technology (based on patent classification)

Table 2: CPC 2-digit sections (based on technologies)

A0: Agriculture	D2: Paper
A2: Foodstuffs; Tobacco	E0: Building
A4: Personal or domestic articles	E2: Earth drilling; Mining
A6: Health; Amusement	F0: Engines or pumps
B0: Separating; Mixing	F1: Engineering in general
B2/B3: Shaping	F2: Lighting; Heating
B4: Printing	F4: Weapons; Blasting
B6: Transporting	G0/G1: Instruments
B8: Microstructural technology; Nanotechnology	G2: Nucleonics
C0/C1: Chemistry	H0: Electrics and electronics
C2/C3: Metallurgy	H1: Semiconductor devices; Electric solid-state devices not otherwise provided for
C4: Combinatorial technology	Y0: General tagging of new technological developments
D0/D1: Textiles or flexible materials not otherwise provided for	Y1: Technical subjects covered by former USPC

When viewed at a more granular level of patent subclasses (CPC-4 digit), as in Figure 3 below, exposure is not uniform across technologies as measure by patent class as the distribution is skewed. Many patent subclasses have very little exposure, but there are some patent subclasses with high exposure. The top ten classes by exposure are generally in the fuel and medical industries. They are, in descending order, (descriptions simplified for brevity): C10B: Destructive Distillation of Carbonaceous Materials, C06F: Pyrotechnic Devices, C10L: Fuels Not Otherwise Provided For, C10G: Hydrocarbon Oils, C07J: Steroids, C07D: Heterocyclic Compounds, C07K: Peptides, A61K: Preparations for Medical, Dental, or Toilet Purposes, A61J: Containers and Devices Specially Adapted for Medical or Pharmaceutical Purposes, A61M: Devices for Introducing Media into, or Onto, the Body and for Sleep. This fits with arguments the energy sector is experiencing high levels of knowledge leakage (Sumanadasa, 2018). It is also in keeping with research that suggests pharmaceutical and medical device industries are particularly heavy users of trade secrets (Gibbons and Vogel, 2007).

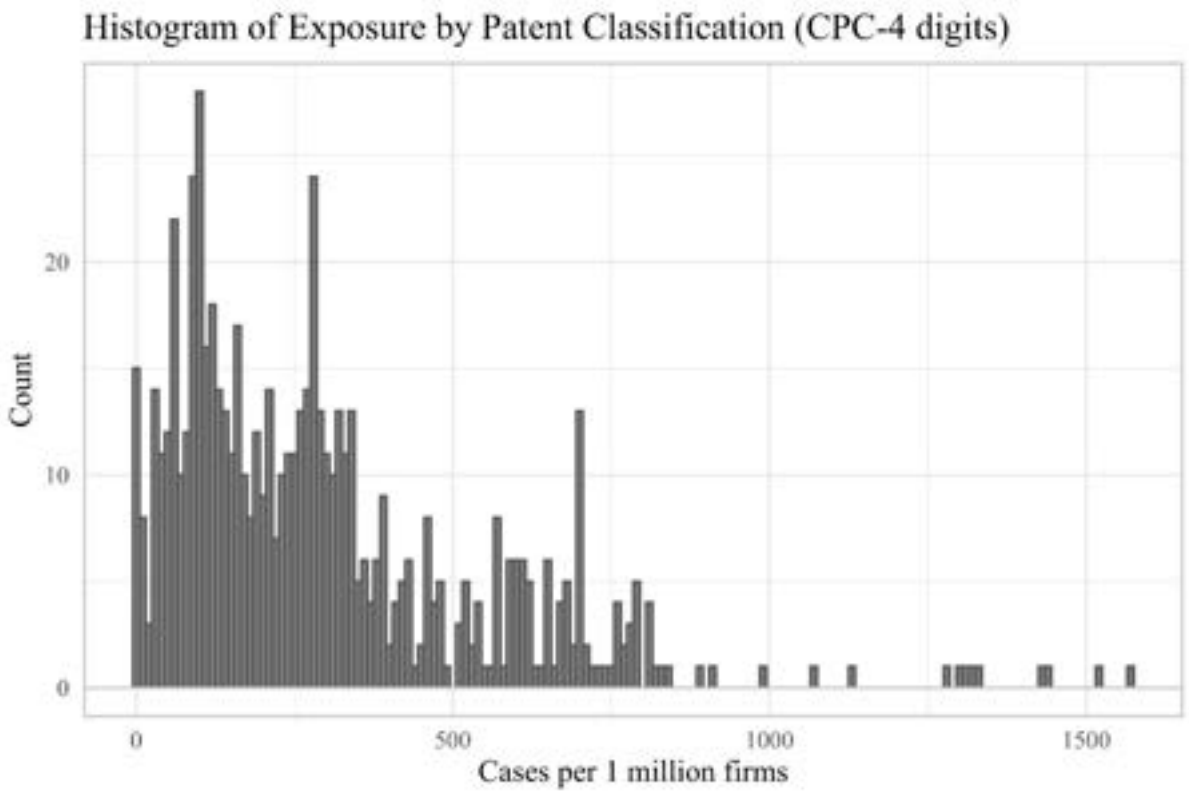

Figure 3: Histogram of Knowledge Leakage by Technology (based on patent classification)

Next, we looked at knowledge leakage by industries through the lens of sensitive economic areas, which enables us to add an economic and national security angle to the analysis.

Turning to the 17 sensitive economic areas, the analysis indicates there is a difference between sensitive and non-sensitive economic areas. Statistical analysis find that sensitive

economic areas were, on average, 17.6%[14] more exposed to knowledge leakage than non-sensitive areas. While more research is needed to understand the causes and mechanisms behind this, that sensitive economic areas are more exposed to knowledge leakage underlines one aspect of why they are sensitive – when compromised, activity in these areas can have negative impacts on national security.

Of the sensitive economic areas, as per Figure 4, Synthetic Biology is the one most exposed to knowledge leakage in our data, with cases in this industry area nearly double those of non-sensitive areas. Synthetic biology is a highly interdisciplinary field that often requires collaborations (Hallinan et al., 2019) and likely has higher-than-average knowledge flows, which are associated with higher levels of knowledge leakage. Additionally, informal discussions with experts suggest that IP awareness varies by discipline, and it may be that Synthetic Biology has a relatively low understanding of IP.

As we were unable to identify research investigating differences between the instance of knowledge leakage in sensitive and non-sensitive areas, we believe our findings here are a first.

[14] A two-sided t-test of difference between means of exposure is statistically significant at the 1% level. Where mean(non-sensitive) = 40.25, mean(sensitive) = 47.33, tstat(2-sided) = -2.76, p-value 0.01.

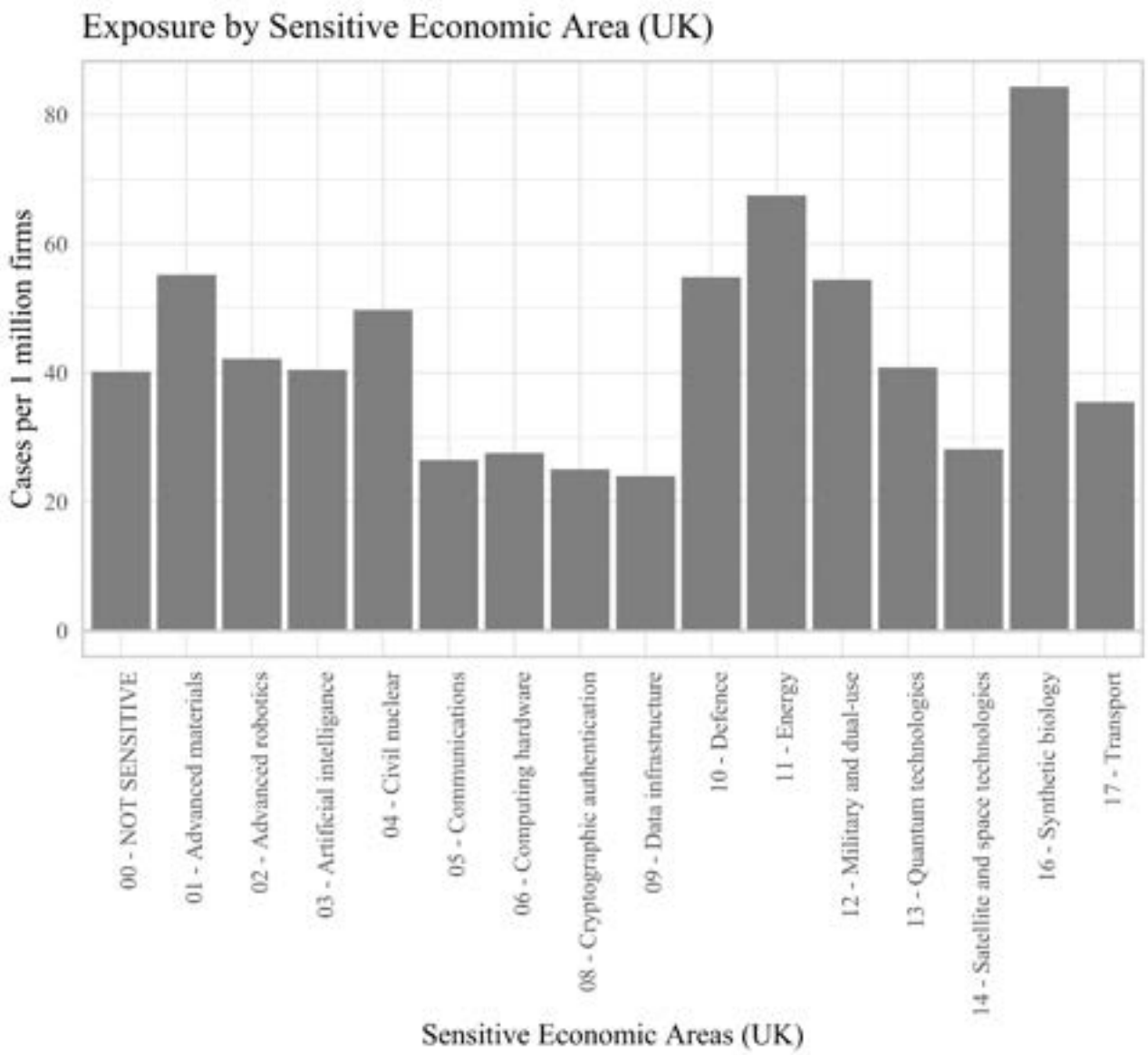

Figure 4: Knowledge Leakage by Industry in Sensitive Economic Areas

Looking at how knowledge leakage develops over time, there is an indication that sensitive economic areas had significant growth in knowledge leakage in the pre-pandemic years (see Figure 5 below.) This is the case both with the date when the case is filed (filing year), which peaks in 2020, and when the case concludes (judgement year) in 2021. We note two caveats to this figure. First, the data collection for the knowledge leakage cases captures a relatively larger portion of more recent cases as it looks at cases concluded from 2017 through 2022. Second, the steep drop-off following the onset of the Covid pandemic is likely attributed to pandemic-related decreases economic and legal activity, rather than a shift in knowledge leakage. However, the pre-2020/21 trajectory is in keeping with informal discussions with experts that indicate knowledge leakage cases are increasing.

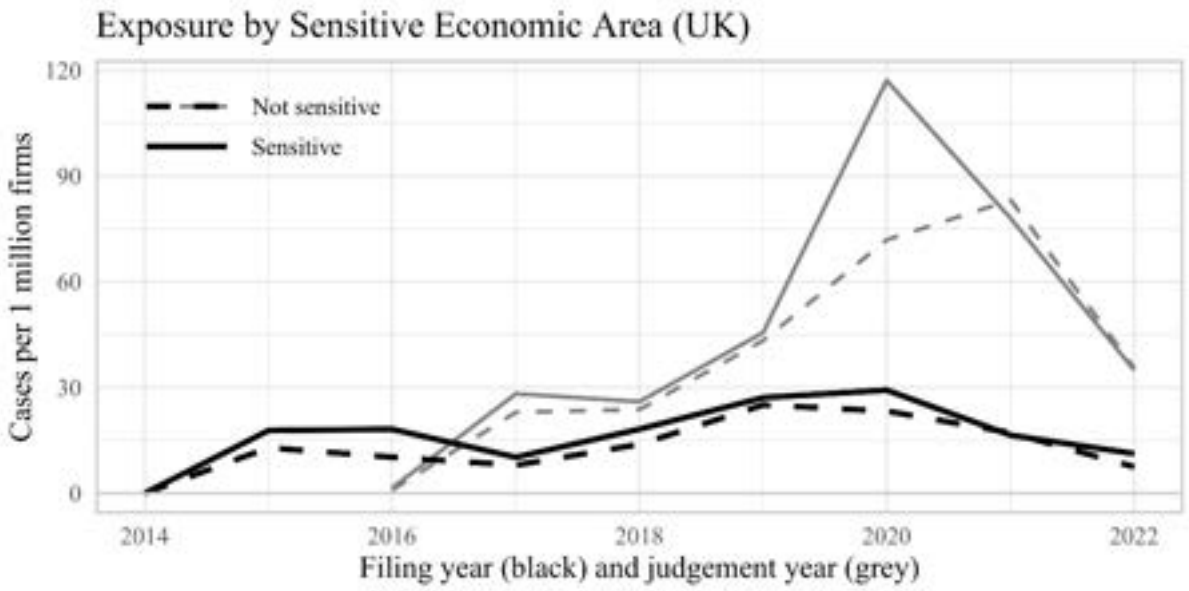

Figure 5: Knowledge Leakage by Industry Over Time (Sensitive Vs. Non-Sensitive)

Our next step was to look at patenting behaviour as related to knowledge leakage. Figure 6 shows the relative change in patent applications, scaled to 2014 application counts, by tercile of knowledge leakage exposure.[15] Interestingly, the order, from biggest to smallest by both exposure and patent applications generally matches. Patent applications in high exposure industries are generally higher and have grown faster than in low and medium exposure technologies. Technologies in low exposure industries are associated with lower levels of patenting.

There are several potential explanations for this. One explanation is that firms in industries with high exposure are more likely to patent to prevent knowledge leakage, as the patent provides legal protections a leaked trade secret cannot. However, an alternative explanation is that industries that use patents more heavily are both heavier users of all types of IP rights and more IP rights aware (Crass et al., 2019). The knowledge leakage cases cover trade secrets, and the patent applications are associated with patents. The firm may be both more likely to use trade secrets and more likely to be aware, protect, monitor and litigate those secrets.

[15] There are historical dips in patent applications following the 2007 financial crisis and the 2020 pandemic.

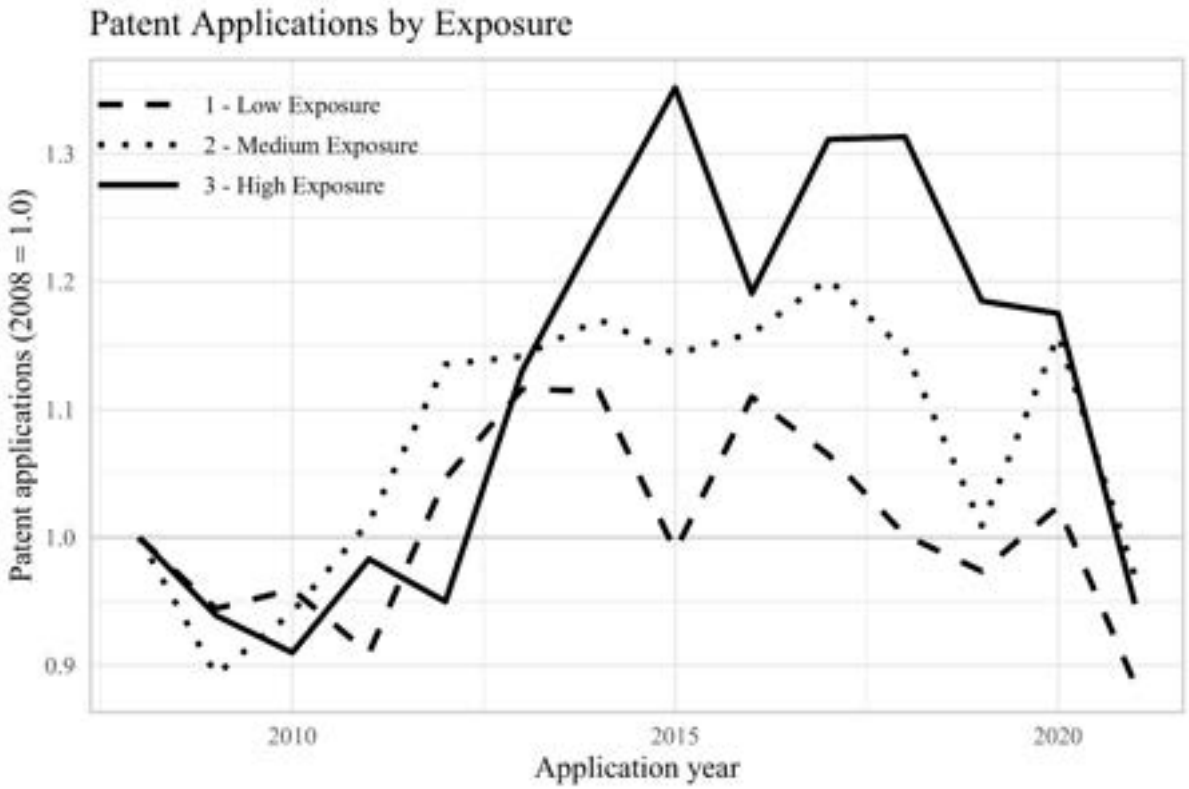

Figure 6: Patent Applications by Tercile of Knowledge Leakage by Industry, Relative To 2008 Patent Applications

To capture patent application growth rates, we then looked at patent applications by decile of knowledge leakage exposure, where 1 is the lower exposure industries and 10 the highest. Figure 7 shows the growth rates (2009-2021) across the deciles. The fitted line indicates a positive relationship between knowledge exposure and patenting, with patenting increasing as exposure rises. Technologies in higher exposure industries have had higher patent application growth rates than those that those with lower knowledge leakage exposure. As this is a measure of growth rates, rather than the absolute number of applications, it more strongly points to a relationship between knowledge leakage and patent applications. While it is not explicit support for a causal relationship, it suggests that higher exposure may lead to higher patenting. Equally, knowledge leakage and patent applications may be positively correlated with high-growth industries. IP in 'hot' technologies may be more desirable and highly innovative, hence higher patenting levels and more interesting IP for intentional knowledge leakage.

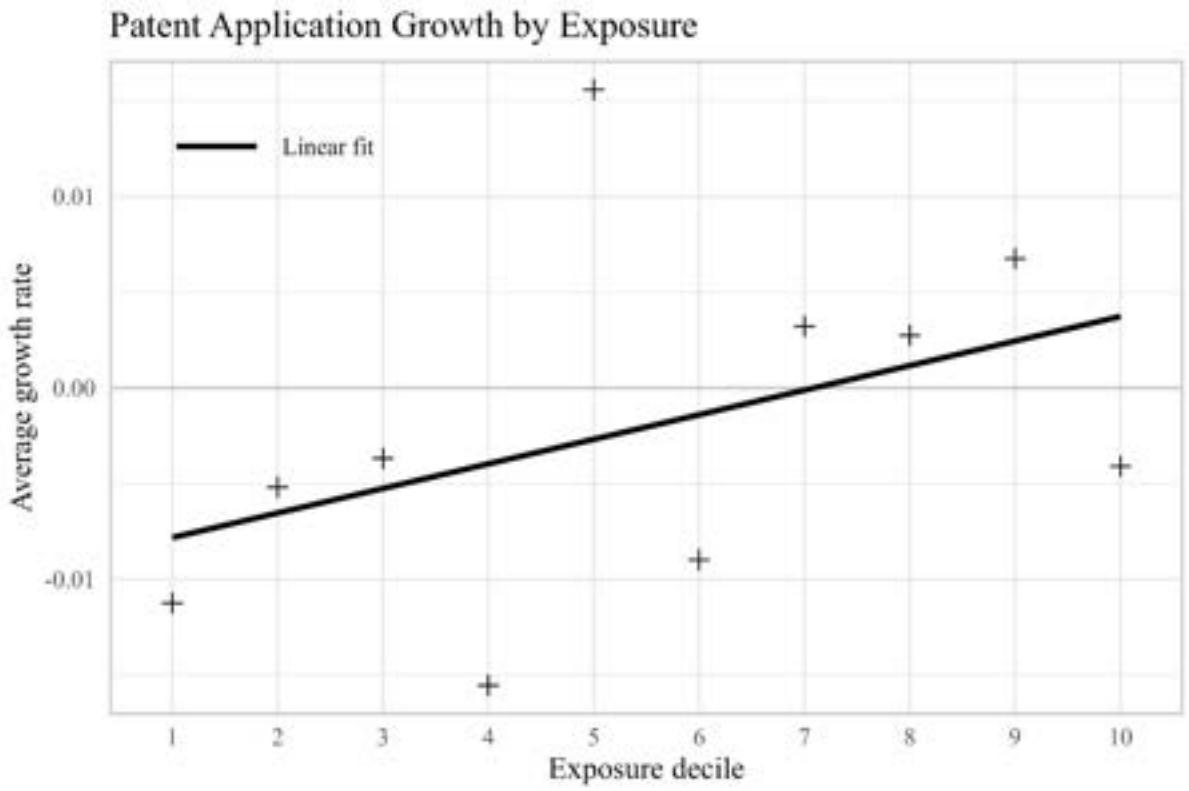

Figure 7: Patent Application Growth Rates (2009-2021) by Knowledge Leakage by Industry Decile

Finally, we look at our measure of the choice of knowledge disclosure, patenting, separated by sensitive and not-sensitive economic areas. There is limited research comparing the knowledge protection practices of sensitive to non-sensitive economic areas. For example, there is a lack of consensus on whether patents for military technologies behave similarly to those of civilian technologies in knowledge flows (Acosta et al., 2013; Schmid, 2018).

Our analysis indicates sensitive economic areas are more active in patenting than non-sensitive economic areas. Sensitive economic areas apply for patents at four times the average of their non-sensitive counterparts.[16] However, this should be interpreted with the strong caveat that patenting rates vary across industries and types of innovations; we would expect the product-intense industries that fall under sensitive economic areas to be heavier users of patents (as patents are more commonly used for products and not services (Brouwer and Kleinknecht, 1999)).

Given that the sensitive economic areas identified by the UK government have important national and economic security concerns, and therefore are potentially in global innovation races, it follows that these firms would want patents to provide protection against knowledge leakage. On the other hand, there are circumstances in which firms in these industries are

[16] A two-sided t-test of the difference between the mean number of patent applications by CPC 4-digit subclass is statistically significant at the 1% level. Where mean (non-sensitive = 38.70, mean(sensitive) = 166.27, t-stat(2-sided) = -31.29 and p-value 0.00

restricted from patenting for national security reasons (i.e. under laws such as the UK's Official Secrets Act), which would suggest these industries would have lower levels of patenting. At the moment, the data does not allow us to do a like-for-like comparison, so we suggest caution with the interpretation of these results.

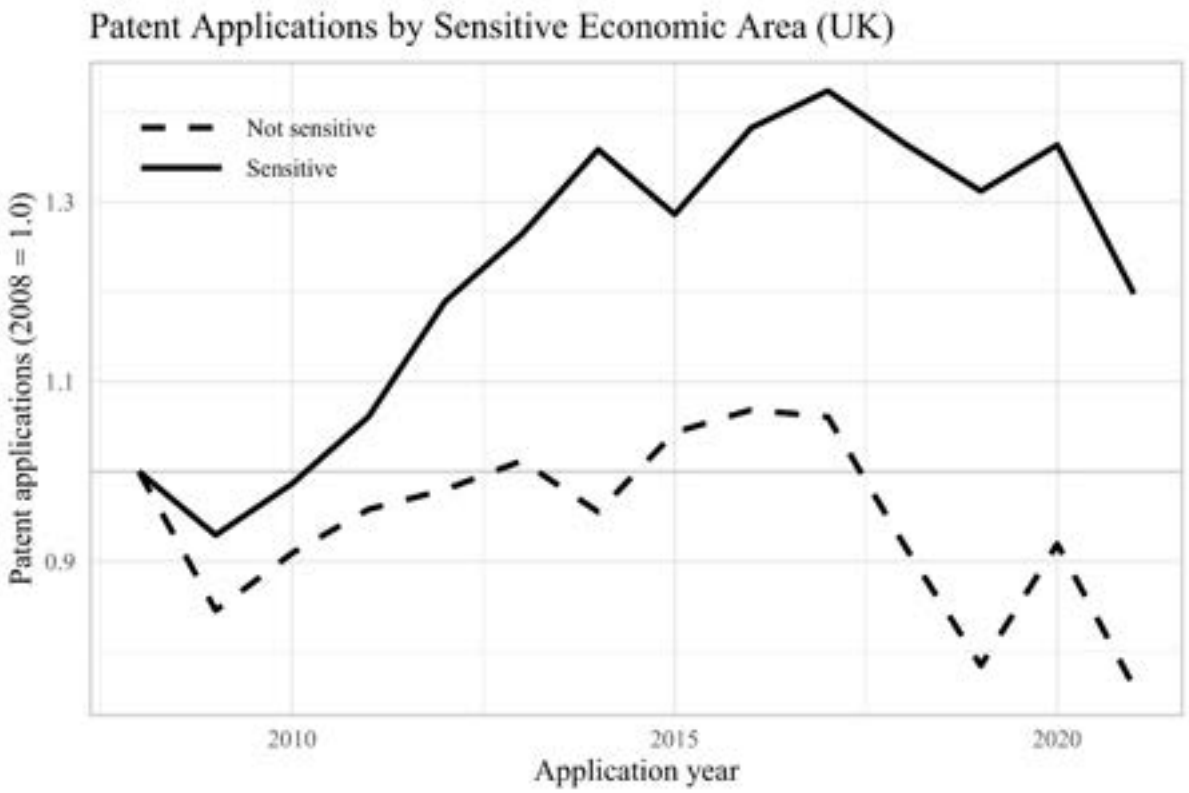

Figure 8: Disclosure Behaviour Comparing Sensitive Economic Areas and Not Sensitive, Relative To 2008 Patent Applications

As an exploratory analysis, including a visual analysis, summary statistics and comparisons between means, the analysis here[17] suggests there are significant differences between industries (in keeping with research indicating different protection strategies across industries (Brouwer and Kleinknecht, 1999; Chabchoub and Niosi, 2005)). Some industries are particularly exposed to knowledge leakage, and the analysis confirms sensitive economic areas are more prone to knowledge leakage than non-sensitive areas. It is quite clear the sensitive economic areas are much more active in patenting, which, to return to our discussion on disclosure, is a decision to disclose knowledge. While it is somewhat counterintuitive that industries that are identified as relevant to the TRI government agenda, in that these industries are singled out due to their economic and national security

[17] Causal analysis will be addressed in future work.

relevance, would deliberately disclose their knowledge, it may be that this thwarts knowledge leakage.

We believe this is the first piece of research to look at knowledge leakage, disclosure and economic & national security. Our finding that industries with higher levels of exposure to knowledge leakage also more heavily patent is in keeping with existing research findings that firms rely on patents in the face of knowledge leakage (Bhattacharya and Guriev, 2006; Kang and Lee, 2022). We add to this interpretation by finding industries with higher levels of knowledge leakage also disclose, via patents, higher levels of knowledge. Our results here suggest there are differences between industries and exposure to knowledge leakage, where sensitive economic areas are more exposed than non-sensitive. Sensitive economic areas are also heavier users of the patent system compared to non-sensitive, which suggests a difference in disclosure strategies. This furthers the findings of existing research investigating how patents for military technologies differ from civilian technologies (Acosta et al., 2013; Schmid, 2018). What our analysis here does not confirm is the potential causal link between knowledge leakage and disclosure. These preliminary findings suggest there is a relationship, and one that is worth exploring further.

5. Conclusion & Implications

Exploring the policy context, our understanding of knowledge leakage and an empirical analysis of knowledge leakage, this report has set out the foundations to better understand how knowledge works under a TRI lens. While the academic literature indicates knowledge leakage largely stems from the movement of employees and collaborations, there is limited research and evidence investigating the broader research security narrative that emphasises external threats and intentional knowledge leakage. And while we have some understanding on how firms choose to protect their knowledge, there is minimal research on the efficacy of knowledge protection mechanisms in the face of knowledge leakage.

Policy solutions for knowledge leakage aspects of TRI are not obvious. Developing policies that address and balance national and economic security concerns, protection against knowledge leakage, support for knowledge flows and the need for innovation is not an easy task. Thus far, policy has focused on command-and-control policies (e.g. regulations related to exports, focus on specific economic areas), explicitly limiting knowledge flows via (e.g. enhanced vetting of collaborations with specific countries and restricting licensing), support (e.g. awareness raising and compliance support) and IP protection mechanisms. This section revisits these policies in light of our analysis and discusses the resulting implications.

5.1 Targeting Technologies: Command and Control

Command and control policies, which set explicit rules and standards targeting research, restrict knowledge flows indirectly. The clearest TRI example of command and control is the focus on the 17 sensitive economic areas under the 2021 NSI Act. These allow policy to strategically target technologies that are particularly sensitive for UK economic and national security concerns. Our analysis focuses on the economic security aspects of sensitive economic areas, and finds these areas, compared to non-sensitive areas, are more exposed to knowledge leakage and heavier users of disclosure via patents as one means to safeguard knowledge. In addition to their national security aspects, that these areas are more vulnerable to knowledge leakage indicates the targeting of these areas may be appropriate. There are suggestions that sensitive areas may behave differently in terms of innovation (Acosta et al., 2013; Schmid, 2018), however overall we found little research on how knowledge leakage works in this context.[18] Our analysis is a snapshot of the current picture, *better understanding of knowledge leakage in sensitive economic areas could be valuable for developing more targeted strategies.*

[18] In addition, we likely have an incomplete understanding of sensitive areas as information may not be made public for security reasons.

Command and control policies impose additional regulations, which result in increased costs for research. This includes more extensive due diligence procedures (e.g. vetting collaborators and staff), compliance with regulations (e.g. following export control restrictions) and the extensive resources required to maintain audit trails. The more researchers must dedicate resources to following regulations, the fewer resources can be used for innovation (Blind, 2012). That universities have an average of 18 full-time members of staff dedicated to complying with university regulations (including TRI regulations) (Kernohan, 2023), and TRI due diligence costs are roughly £10M per year (Johnson et al., 2023), already suggests considerable opportunity costs. A first step in assessing the impact on innovation of these regulations is to calculate the additional costs associated with them, which should be followed by estimating the benefits of the regulations, such as trust and reputational benefits. *Conducting a cost-benefit analysis of TRI regulations on innovation could provide insights into their overall impact and inform future policy.*

5.2 Managing Knowledge Flows: Restrictions

Policies aimed reducing knowledge flows fall under two areas – limiting collaborations and limiting licensing, both of which are known sources of leakage (Hannah, 2005). In the UK, under current approaches, this involves enhanced scrutiny of overseas researchers coming to the UK and of collaborations with overseas research partners. These fall under national security laws and immigration laws, in particular the ATAS scheme's focus on sensitive research subjects. For example, 1,100 Chinese visa applications were denied to researchers and students in 2022 under ATAS (Das, 2023). Another approach is to not provide public funding for collaborations with overseas partners, as, for example, in the UK's decision to stop funding a China-UK university collaboration scheme (Central Chronicle, 2024). While it is difficult to separate the geopolitical, national security and innovation aspects of these schemes, *developing the evidence base on the impact of restrictions arising from TRI and TRI-adjacent policies on international collaborations and highly skilled labour could provide insights for policymaking.*

Knowledge flows can also be restricted by targeting the licensing of knowledge of knowledge. Licensing is an important source of knowledge flows (Grindley and Teece, 1997) and a common way for innovators (particularly universities) to generate research revenue. As a policy, this falls under the remit of the licensing of IP rights. Our analysis finds sensitive economic areas are more reliant on patents than non-sensitive areas. From a practical perspective, restricting licensing is a difficult policy to implement as it involves the government limiting owners of these property rights to create value[19]. While the UK has regulations in place allowing the restriction of licensing or sale of technologies, these apply

[19] There is precedent for restricting the dissemination of IP rights with national security concerns - as for example the UK Patents Act 1977, Section 22 and the US Invention Secrecy Act of 1951, which allow governments to block or restrict the publication of patent details related to technologies with national security concerns.

to licensing and sales posing security concerns (e.g. the NSI). Extending this security approach to protect against knowledge leakage related to other technologies concerns poses several problems. On a practical level, IP rights are legal rights and restricting them would likely be in breach of national law and international agreements. On a more strategic level, IP licensing is an important mechanism for capturing value and enabling knowledge flows, limiting these knowledge flows – which already occur within a legally protected framework – is likely a disproportionate response. *Extending IP licensing restrictions may have unintended and counterproductive consequences.*

5.3 Awareness and Support

Support and awareness are 'softer', typically cost-effective policies in contrast to 'harder' command-and-control approaches. By providing education, guidance and support, these softer policies can complement or substitute harder regulations. Softer policies can be particularly helpful in influencing organisational culture as a crucial determinant of organisational innovativeness (Martins and Terblanche, 2003). TRI education and compliance support, as offered by UKRI, UUK and ARMA, are examples of these softer policies. UKRI as a non-departmental public body works closely with government and promotes awareness of TRI across the sector to help manage TRI risks and to influence research security culture. It adopts a risk-assessed approach to its investments and activities to enable collaborations to be done safely and securely. More broadly, organisations such as UUK and ARMA are supporting the development of TRI policy and practices across the R&I ecosystem. Support also comes from HEECA, which seeks to 'develop, maintain and promote best practice' in export compliance in UK universities, in addition to dedicated UK government support (e.g. RCAT). *Maintaining existing TRI support activities, and periodically evaluating them, could help ensure they continue to meet evolving needs*[20].

As employer–employee trust and understanding are important for protections against the largest source of knowledge leakage - employees (Almeling et al., 2009; Hannah, 2005; Hannah and Robertson, 2015), awareness and support should be effective in supporting a R&I ecosystem culture that protects against knowledge leakage. A challenge is that job insecurity undermines trust and innovation (Martins and Terblanche, 2003; Hannah, 2005; Reder and O'Brien, 2011; Wang, 2021). At the time of writing, UK job insecurity is increasing (Florisson, 2024) and job losses are underway across the HEI sector. A loss of trust in the R&I ecosystem could result in higher levels of knowledge leakage. Job insecurity raises job mobility, and as employees move between jobs, they increase knowledge flows but also leakage. Additionally, leaving employment distances the employee from the research security mechanisms of their former employer. In the context of a changing work

[20] Many organisations already do this. UKRI, for example, already regularly evaluates its approach to TR&I as required by its role as a non-departmental public body.

environment, softer policies addressing culture and trust are particularly important. *Exploring how policies can foster trust and TRI-positive cultures could inform the development of softer policies that provide effective complements to harder policies.*

5.4 IP Management Strategies

IP rights enable firms to profit from their knowledge. As discussed in our analysis of knowledge leakage and patents, knowledge leakage cannot strictly occur when patents are used to protect knowledge. In practice, plenty of knowledge surrounding the patent can leak. Firms typically use bundles of IP rights to protect their knowledge, several of which do not address knowledge leakage (such as copyright and trade marks).

Identifying the best IP protection strategy for knowledge under the threat of knowledge leakage is a challenge (Bhattacharya and Guriev, 2006; Kang and Lee, 2022). While patents may provide refuge, the effectiveness of this varies by discipline and type of knowledge (Brouwer and Kleinknecht, 1999; Chabchoub and Niosi, 2005). Outside of STEM disciplines, there is minimal knowledge generation that could lead to patents, although other types of IP rights, namely copyright, may be relevant. Yet, that which cannot be patented may still be leaked. Our research indicates there may be a relationship between knowledge leakage and firms' choice of IP protections strategy. *Exploring how IP management strategies can protect against knowledge leakage, and investigating how this varies by discipline, industry, or technology, could aid the development of practical approaches to knowledge leakage management.*

Knowledge sharing, and by consequence leakage, is part of academic culture. Employee and employer incentives are misaligned. Universities and governments expect to profit from employee-generated IP, while employees' careers are dependent on developing and disclosing their personal body of knowledge (Dietz and Bozeman, 2005; Blind et al, 2018). University patenting, as a means to profit from IP and manage knowledge leakage, conflicts with researchers' career incentives as patenting requires the knowledge not be publicly disclosed before the patent is filed. This puts an employee's ability to publish in competition with their employer's ability to patent. Asking academics to put patents before publications is asking academics to compromise their career success as it delays academic publications. This misalignment of incentives is also reinforced beyond the university system (e.g. external evaluations of university productivity). *Aligning incentives between universities and their employees could support joint efforts to prevent knowledge leakage.*

There is a wider question over the conflicting goals of public research as an engine for knowledge creation and knowledge flows, versus pressures on universities to control and profit from their knowledge. Universities should simultaneously create social value and economic value, where social value creation is associated with higher levels of knowledge flows (De Silva and Wright, 2019). This creates a knowledge flow paradox for publicly funded research organisations as it is not clear at what point encouraging knowledge flows

becomes encouraging undesirable knowledge leakage that compromises the organisation's ability to profit (Ritala et al, 2015). Universities are in the middle of this tension as they are expected to encourage knowledge flows. We do not think there is a straightforward answer to this paradox. *Further reflection on how universities define undesirable knowledge leakage may clarify their innovation and innovation-protection strategies.*

The implications of our analysis can be summarised under three themes for potential action: research, regulation, and refinement. More broadly, we call for better understanding of the balance between protecting against knowledge leakage and encouraging knowledge flows.

Now you have read our report we would love to know if our research has provided you with new insights, improved your processes, or inspired innovative solutions.

Please let us know how our research is making a difference by completing our short feedback form via this QR code.

Thank you

The Innovation & Research Caucus

References

Acosta, M., Coronado, D., Marín, R., Prats, P., 2013. Factors affecting the diffusion of patented military technology in the field of weapons and ammunition. Scientometrics 94, 1–22. https://doi.org/10.1007/s11192-012-0857-8

Adler, N., Hashai, N., 2007. Knowledge flows and the modelling of the multinational enterprise. Journal of International Business Studies 38, 639–657.

Alberti, F.G., Pizzurno, E., 2017. Oops, I did it again! Knowledge leaks in open innovation networks with start-ups. European Journal of Innovation Management 20, 50–79. https://doi.org/10.1108/EJIM-11-2015-0116

Almeling, D.S., Snyder, D.W., Sapoznikow, M., 2009. A statistical analysis of trade secret litigation in federal courts. Gonz. L. Rev. 45, 291.

Almeling, D.S., Snyder, D.W., Sapoznikow, M., McCollum, W.E., 2010. A statistical analysis of trade secret litigation in state courts. Gonz. L. Rev. 46, 57.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J.G., Levi, M., Moore, T., Savage, S., 2013. Measuring the cost of cybercrime, in: The Economics of Information Security and Privacy. Springer, pp. 265–300.

Andrenelli, A., Gourdon, J., Moïsé, E., 2019. International Technology Transfer Policies. OECD Trade Policy Papers 222.

Arias-Pérez, J., Lozada, N., Henao-García, E., 2020. When it comes to the impact of absorptive capacity on co-innovation, how really harmful is knowledge leakage? Journal of Knowledge Management 24, 1841–1857. https://doi.org/10.1108/JKM-02-2020-0084

Aydinliyim, L.E., 2022. The Case for Ethical Non-compete Agreements: Executives Versus Sandwich-Makers. J Bus Ethics 175, 651–668. https://doi.org/10.1007/s10551-020-04570-w

Bahar, D., Choudhury, P., Rapoport, H., 2020. Migrant inventors and the technological advantage of nations. Research Policy 49, 103947.

Bhattacharya, S., Guriev, S., 2006. Patents vs. Trade Secrets: Knowledge Licensing and Spillover. Journal of the European Economic Association 4, 1112–1147. https://doi.org/10.1162/JEEA.2006.4.6.1112

Blind, K., 2012. The influence of regulations on innovation: A quantitative assessment for OECD countries. Research policy, 41(2), pp.391-400.

Blind, K., Pohlisch, J. and Zi, A., 2018. Publishing, patenting, and standardization: Motives and barriers of scientists. Research Policy, 47(7), pp.1185-1197.

Borghi, M., Cogo, A., Khan, B., 2023. Trade Secrets Litigation Trends in the EU. https://doi.org/10.2814/565721

Bozeman, B., 2000. Technology transfer and public policy: a review of research and theory. Research Policy 29, 627–655. https://doi.org/10.1016/S0048-7333(99)00093-1

Bozeman, B., Rimes, H., Youtie, J., 2015. The evolving state-of-the-art in technology transfer research: Revisiting the contingent effectiveness model. Research Policy 44, 34–49. https://doi.org/10.1016/j.respol.2014.06.008

Breschi, S., Lissoni, F., 2009. Mobility of skilled workers and co-invention networks: an anatomy of localized knowledge flows. Journal of Economic Geography 9, 439–468. https://doi.org/10.1093/jeg/lbp008

Brouwer, E., Kleinknecht, A., 1999. Innovative output, and a firm's propensity to patent.: An exploration of CIS micro data. Research Policy 28, 615–624. https://doi.org/10.1016/S0048-7333(99)00003-7

Central Chronicle, 2024. UK fully stops funding China-backed Confucius Institutes in country. URL https://www.centralchronicle.com/uk-fully-stops-funding-china-backed-confucius-institutes-in-country/ (accessed 12.19.24).

Chabchoub, N., Niosi, J., 2005. Explaining the propensity to patent computer software. Technovation 25, 971–978. https://doi.org/10.1016/j.technovation.2004.02.015

Chubb, A., Cooney-O'Donoghue, D., Shih, T., 2023. Closed countries, open science. Research Professional News. URL https://www.researchprofessionalnews.com/rr-news-uk-views-of-the-uk-2023-8-closed-countries-open-science/ (accessed 6.20.24).

Cole, E., Ring, S., 2005. Insider threat: Protecting the enterprise from sabotage, spying, and theft. Elsevier.

Crass, D., Garcia Valero, F., Pitton, F., Rammer, C., 2019. Protecting Innovation Through Patents and Trade Secrets: Evidence for Firms with a Single Innovation. International Journal of the Economics of Business 26, 117–156. https://doi.org/10.1080/13571516.2019.1553291

Das, M., 2023. Students and researchers from China barred from working in the UK. The Lancet Oncology 24, 434. https://doi.org/10.1016/S1470-2045(23)00143-2

David, M., Halbert, D., 2015. Owning the world of ideas: Intellectual property and global network capitalism. Sage.

De Silva, M. and Wright, M., 2019. Entrepreneurial co-creation: societal impact through open innovation. R&D Management, 49(3), pp.318-342.

Dietz, J.S. and Bozeman, B., 2005. Academic careers, patents, and productivity: industry experience as scientific and technical human capital. Research policy, 34(3), pp.349-367.

Directorate General for Research and Innovation, 2024. EU Member States adopt recommendations to enhance research security - European Commission [WWW Document]. URL https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/eu-member-states-adopt-recommendations-enhance-research-security-2024-05-23_en (accessed 3.6.25).

Dreyfuss, R.C., Lobel, O., 2016. Economic espionage as reality or rhetoric: Equating trade secrecy with national security. Lewis & Clark L. Rev. 20, 419.

Edler, J., Fier, H., Grimpe, C., 2011. International scientist mobility and the locus of knowledge and technology transfer. Research Policy 40, 791–805. https://doi.org/10.1016/j.respol.2011.03.003

Effron, R.J., 2016. Trade Secrets, Extraterritoriality, and Jurisdiction. Wake Forest L. Rev. 51, 765.

Ferenhof, H.A., 2016. Recognizing knowledge leakage and knowledge spillover and their consequences. International Journal of Knowledge and Systems Science (IJKSS) 7, 46–58.

Florisson, R., 2024. The UK Insecure Work Index 2024 [WWW Document]. Lancaster University. URL https://www.lancaster.ac.uk/work-foundation/publications/the-uk-insecure-work-index-2024 (accessed 12.19.24).

Frishammar, J., Ericsson, K., Patel, P.C., 2015. The dark side of knowledge transfer: Exploring knowledge leakage in joint R&D projects. Technovation 41, 75–88.

Furman, J.L., Nagler, M., Watzinger, M., 2021. Disclosure and Subsequent Innovation: Evidence from the Patent Depository Library Program. American Economic Journal: Economic Policy 13, 239–270. https://doi.org/10.1257/pol.20180636

G20 Leaders, 2015. G20 Leaders' Communiqué, Antalya Summit.

Gabel, T., 2024. Germany mulls new research security organisation | Science|Business [WWW Document]. URL https://sciencebusiness.net/news/germany-mulls-new-research-security-organisation (accessed 3.6.25).

Ganglmair, B., Holcomb, A., Myung, N., 2020. Expectations of reciprocity when competitors share information: Experimental evidence. Journal of Economic Behavior & Organization 170, 244–267. https://doi.org/10.1016/j.jebo.2019.12.006

Ganglmair, B., Tarantino, E., 2014. Conversation with secrets. The RAND Journal of Economics 45, 273–302.

Gibbons, R.G., Vogel, B.J., 2007. The Increasing Importance of Trade Secret Protection in the Biotechnology, Pharmaceutical and Medical Device Fields. J. Pat. & Trademark Off. Soc'y 89, 261–286.

Glitz, A., Meyersson, E., 2020. Industrial espionage and productivity. American Economic Review 110, 1055–1103.

Grinblatt, M., Keloharju, M., 2001. How Distance, Language, and Culture Influence Stockholdings and Trades. The Journal of Finance 56, 1053–1073. https://doi.org/10.1111/0022-1082.00355

Grindley, P.C., Teece, D.J., 1997. Managing Intellectual Capital: Licensing and Cross-Licensing in Semiconductors and Electronics. California Management Review 39, 8–41. https://doi.org/10.2307/41165885

Gross, D.P., 2023. The Hidden Costs of Securing Innovation: The Manifold Impacts of Compulsory Invention Secrecy. Management Science 69, 2318–2338. https://doi.org/10.1287/mnsc.2022.4457

Hallinan, J.S., Wipat, A., Kitney, R., Woods, S., Taylor, K., Goñi-Moreno, A., 2019. Future-proofing synthetic biology: educating the next generation. Engineering Biology 3, 25–31. https://doi.org/10.1049/enb.2019.0001

Hannah, D.R., 2005. Should I Keep a Secret? The Effects of Trade Secret Protection Procedures on Employees' Obligations to Protect Trade Secrets. Organization Science 16, 71–84. https://doi.org/10.1287/orsc.1040.0113

Hannah, D.R., Robertson, K., 2015. Why and how do employees break and bend confidential information protection rules? Journal of Management Studies 52, 381–413.

Hegde, D., Herkenhoff, K., Zhu, C., 2023. Patent Publication and Innovation. Journal of Political Economy 131, 1845–1903. https://doi.org/10.1086/723636

Hegde, D., Luo, H., 2017. Patent Publication and the Market for Ideas. Management Science. https://doi.org/10.1287/mnsc.2016.2622

Hellmann, T., Perotti, E., 2011. The Circulation of Ideas in Firms and Markets. Management Science 57, 1813–1826. https://doi.org/10.1287/mnsc.1110.1385

Hughes, M., Mercer, S., Harris, A., Benzie, A., Williams, S., Kenneison, E., 2025. Securing the UK's AI Research Ecosystem. The Alan Turing Institute.

Inkpen, A., Minbaeva, D., Tsang, E.W.K., 2019. Unintentional, unavoidable, and beneficial knowledge leakage from the multinational enterprise. Journal of International Business Studies 50, 250–260. https://doi.org/10.1057/s41267-018-0164-6

Innovate UK, 2020. Securing the integrity of international research collaborations - Innovate UK. Innovate UK Blog. URL https://webarchive.nationalarchives.gov.uk/ukgwa/20210728192958oe_/https://innovateuk.blog.gov.uk/2020/09/10/securing-the-integrity-of-international-research-collaboration/ (accessed 6.20.24).

Johnson, J., Marwaha, S., Dickson, L., Timlin, J., Kagiri-Kalanzi, E., 2023. Complex Collaborations – Efficiency, Equity, Quality and Security in International Research. Association of Research Managers and Administrators (ARMA).

Kang, H., Lee, W., 2022. How innovating firms manage knowledge leakage: A natural experiment on the threat of worker departure. Strategic Management Journal 43, 1961–1982. https://doi.org/10.1002/smj.3404

Kernohan, D., 2023. Universities UK counts the cost of regulation. Wonkhe. URL https://wonkhe.com/blogs/universities-uk-count-the-cost-of-regulation/ (accessed 12.19.24).

Kim, A.C., 2018. Prosecuting Chinese Spies: An empirical analysis of the economic espionage act. Cardozo L. Rev. 40, 749.

Kim, K.-S., Cho, N.-W., 2022. A Study on the Improvement of the Defense-related International Patent Classification using Patent Mining. Journal of Korean Society for Quality Management 50, 21–33. https://doi.org/10.7469/JKSQM.2022.50.1.21

Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X., 2021. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security 105, 102248.

Lybbert, T.J., Zolas, N.J., 2014. Getting patents and economic data to speak to each other: An 'Algorithmic Links with Probabilities' approach for joint analyses of patenting and economic activity. Research Policy 43, 530–542. https://doi.org/10.1016/j.respol.2013.09.001

Martins, E.C. and Terblanche, F., 2003. Building organisational culture that stimulates creativity and innovation. European journal of innovation management, 6(1), pp.64-74.

Marwaha, S., 2024. The challenge of pursuing research security when nationality becomes a shorthand for risk. Wonkhe. URL https://wonkhe.com/blogs/the-challenge-of-pursuing-research-security-when-nationality-becomes-a-shorthand-for-risk/ (accessed 6.20.24).

Marwaha, S., 2022. The trusted research agenda demands dedicated resources. Research Professional News. URL https://www.researchprofessionalnews.com/rr-news-uk-views-of-the-uk-2022-11-the-trusted-research-agenda-demands-dedicated-resources/ (accessed 6.20.24).

Marx, M., 2011. The firm strikes back: non-compete agreements and the mobility of technical professionals. American Sociological Review 76, 695–712.

Montobbio, F., Staccioli, J., Virgillito, M.E., Vivarelli, M., 2022. Robots and the origin of their labour-saving impact. Technological Forecasting and Social Change 174, 121122. https://doi.org/10.1016/j.techfore.2021.121122

National Science Foundation, 2023. Dear Colleague Letter: Workshop to Inform Development of the NSF Research on Research Security Program (RRSP) [WWW Document]. URL https://www.nsf.gov/pubs/2023/nsf23126/nsf23126.jsp (accessed 6.20.24).

Oettl, A., Agrawal, A., 2008. International labor mobility and knowledge flow externalities. J Int Bus Stud 39, 1242–1260. https://doi.org/10.1057/palgrave.jibs.8400358

Pathak, S., Xavier-Oliveira, E., Laplume, A.O., 2013. Influence of intellectual property, foreign investment, and technological adoption on technology entrepreneurship. Journal of Business Research 66, 2090–2101. https://doi.org/10.1016/j.jbusres.2013.02.035

Prud'homme, D., von Zedtwitz, M., Thraen, J.J., Bader, M., 2018. "Forced technology transfer" policies: Workings in China and strategic implications. Technological Forecasting and Social Change 134, 150–168. https://doi.org/10.1016/j.techfore.2018.05.022

Reder, M.E.K., O'Brien, C.N., 2011. Managing the risk of trade secret loss due to job mobility in an innovation economy with the theory of inevitable disclosure. J. High Tech. L. 12, 373.

Ritala, P., Olander, H., Michailova, S., Husted, K., 2015. Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. Technovation 35, 22–31. https://doi.org/10.1016/j.technovation.2014.07.011

Roper, S., Hewitt-Dundas, N., 2015. Knowledge stocks, knowledge flows and innovation: Evidence from matched patents and innovation panel data. Research Policy 44, 1327–1340. https://doi.org/10.1016/j.respol.2015.03.003

Sandberg, J., 2015. Human element of corporate espionage risk management: literature review on assessment and control of outsider and insider threats.

Schmid, J., 2018. The Diffusion of Military Technology. Defence and Peace Economics 29, 595–613. https://doi.org/10.1080/10242694.2017.1292203

Searle, N., 2021. The economic and innovation impacts of trade secrets. UK Intellectual Property Office Research Paper.

Shackelford, S.J., 2016. Protecting intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate cyber risk. Chap. L. Rev. 19, 445.

Shackelford, S.J., Sulmeyer, M., Deckard, A.N.C., Buchanan, B., Micic, B., 2017. From Russia with Love: Understanding the Russian Cyber Threat to US Critical Infrastructure and What to Do about It. Neb. L. Rev. 96, 320.

Singh, J., Agrawal, A., 2011. Recruiting for Ideas: How Firms Exploit the Prior Inventions of New Hires. Management Science 57, 129–150. https://doi.org/10.1287/mnsc.1100.1253

Snetselaar, D., Frerks, G., Gould, L., Rietjens, S., Sweijs, T., 2022. NATO Review - Knowledge security: insights for NATO [WWW Document]. NATO Review. URL https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html?utm_source=chatgpt.com (accessed 1.27.25).

Sorenson, O., Rivkin, J.W., Fleming, L., 2006. Complexity, networks and knowledge flow. Research Policy 35, 994–1017. https://doi.org/10.1016/j.respol.2006.05.002

Sumanadasa, D., 2018. Protecting and Promoting Clean Energy Innovation Through the Trade Secrets Regime: Issues and Implications, in: Rimmer, M. (Ed.), Intellectual Property and Clean Energy: The Paris Agreement and Climate Justice. Springer, Singapore, pp. 399–424. https://doi.org/10.1007/978-981-13-2155-9_15

Tan, K.H., Wong, W.P., Chung, L., 2016. Information and Knowledge Leakage in Supply Chain. Inf Syst Front 18, 621–638. https://doi.org/10.1007/s10796-015-9553-6

Turone, F., 2024. Italian research sector recognises security concerns. Research Professional News. URL https://www.researchprofessionalnews.com/rr-news-europe-italy-2024-11-italian-research-sector-recognises-security-concerns/ (accessed 3.6.25).

UKRI, 2024. Trusted research and innovation [WWW Document]. URL https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/ (accessed 11.18.24).

UKRI, 2023. Annual report and accounts 2022 to 2023 [WWW Document]. URL https://www.ukri.org/publications/annual-report-and-accounts/ (accessed 6.20.24).

Universities, U.K., 2020. Managing risks in internationalisation: Security related issues. Universities UK.

Vats, A., 2020. The color of creatorship: intellectual property, race, and the making of Americans. Stanford University Press.

Wall, D.S., 2013. Enemies within: Redefining the insider threat in organizational security policy. Security journal 26, 107–124.

Wang, R., 2021. Information asymmetry and the inefficiency of informal IP strategies within employment relationships. Technological Forecasting and Social Change 162, 120335.

Williams, N., 2024. Foreign states targeting UK universities, MI5 warns. BBC News online.

Appendix

Appendix A: Concordance

Table A1: Matching the 17 Sensitive Economic Areas to their Cooperative Patent Classification (CPC)

Area	Description of Sensitive Economic Areas	Patent subclasses (CPC)
1	Advanced Materials	B29C; B32B; B82B; B82Y; C01B; C03B; C04B; C08J; C08L; C09K; C22C; C22F; G01G; G05F; H01L; H01M
2	Advanced Robotics	A47L; A61B; A61F; A63H; B05B; B21D; B23K; B23P; B23Q; B25J; B60W; B62D; B65G; F22B; G01B; G01L; G01N; G05B; G05D; G06N; G21C; H01L; H05K
3	Artificial Intelligence	B25J; G05B; G05D; G06F; G06K; G06N; G06Q; G06T; G06V; G08G; G10L
4	Civil Nuclear	A61K; A61N; A61P; C09K; C22B; C22C; C22F; F01D; F01K; F03G; G01D; G01J; G01T; G21B; G21C; G21D; G21F; G21G; G21H; G21K; H02J; H02P
5	Communications	G06Q; H01Q; H04B; H04H; H04J; H04L; H04M; H04N; H04Q; H04T
6	Computing Hardware	G06F; G06K; G06N; G06Q; G06T; G09C; G09G; G11C; H01L; H04L; H05K
7	Critical Suppliers to Government	N/A
8	Cryptographic Authentication	G06F; G06Q; G07C; G07F; G09C; G11B; H04L; H04W
9	Data Infrastructure	G06F; G06Q; G06T; G11C; H01L; H04B; H04L; H04W; H05K

Area	Description of Sensitive Economic Areas	Patent subclasses (CPC)
10	Defence	B63G; B64D; C06B; C06C; C06D; F41A; F41C; F41F; F41G; F41H; F41J; F42B; F42C; F42D; G21J; H04K
11	Energy	C10B; C10G; C10J; C10K; C10L; E21B; F01D; F01K; F02C; F02G; F02K; F03D; F03G; F22B; F22D; F22G; H02B; H02G; H02H; H02J; H02K; H02M; H02N; H02P; H02S
12	Military and Dual-Use	B63G; B64D; C06B; C06C; C06D; F23R; F41A; F41B; F41C; F41F; F41G; F41H; F42B; F42C; F42D; G01S; G21J; H01S; H04K
13	Quantum Technologies	B82Y; C09K; G01B; G01N; G02B; G02F; G06N; G06Q; G06T; G09C; H01J; H01L; H01S; H03K; H04B; H04L; H10K
14	Satellite and Space Technologies	B64G; G01S; G01V; G01W; H01Q; H04B; H04L; H04W
15	Suppliers to the Emergency Services	N/A
16	Synthetic Biology	A61K; B82Y; C07K; C12M; C12N; C12P; C12Q; C12Y; C40B; G01N; G06N; G16B
17	Transport	B63B; B63C; B63H; B63J; B64B; B64C; B64D; B64F; B64U; G08G

Appendix B: Glossary

Key terms, policies and entities

ARMA - The Association of Research Managers and Administrators, the UK's professional association for research leadership, management and administration.

ATAS - Academic Technology Approval Scheme, a scheme administered by the UK Foreign & Commonwealth, which monitors research and studies associated with specific technologies with respect to some foreign nationals

Corporate/Industrial Espionage – the act of intentional knowledge leakage

Disclosure – The sharing or publication of information related to innovations

DSIT – The UK Department of Science, Innovation and Technology, DSIT is a ministerial department tasked with supporting UK innovation, investment and productivity setting policy and through its Policy Team and providing advice through RCAT. UKRI and UK IPO are also associated with DSIT.

Economic Espionage – the act of intentional knowledge leakage to benefit foreign entities

FIRS – the Foreign Influence Registration Scheme. The scheme requires individuals and organisations to register their arrangements with foreign powers and certain foreign power-controlled entities where they are directed to carry out certain activities in the UK. FIRS is run by the Home Office.

HEECA - The Higher Education Export Control Association, the national network to develop, maintain and promote best practice in Export Control Compliance across the UK Higher Education sector.

Home Office - The lead government department for immigration and passports, drugs policy, crime, fire, counter-terrorism and police. The Home Office is a ministerial department,

Innovate UK - The UK's innovation agency and part of UKRI.

Innovation – New ideas, products or methods.

Intentional knowledge leakage - the deliberate sharing of confidential knowledge with external parties.

Intellectual Property (IP) - knowledge and innovations, usually resulting from R&D, owned by individuals or organisations.

IP rights - Intellectual property rights, legal protections for IP, including patents, copyrights, trade secrets and trade marks.

Knowledge flows – the movement of knowledge within or between organisations or systems.

Knowledge leakage - the unintended or unauthorised transfer of knowledge to external parties.

NACE - The Statistical Classification of Economic Activities in the European Community, commonly referred to as NACE; the industry standard classification system for economic activities used in the European Union

NPSA - National Protective Security Authority, the government body responsible for physical and personnel protective security. It is associated with the UK Security Service (MI5).

NSA – The National Security Act of 2023

NSF - The National Science Foundation, the US independent federal agency that supports science and engineering in the United States.

NSI - The National Security and Investment Act of 2021

Patent – Legal, intellectual property protection for innovations requiring disclosure of details of innovation

R&I – Research & Innovation

RCAT - Research Collaboration Advice Team, the UK government body providing advice to research institutions on the national security risks linked to international research. RCAT is part of DSIT.

Research – A process that involves knowledge generation and can lead to innovation.

Sensitive Economic Areas – the UK governments named 17 sensitive sectors of the economy that are subject to mandatory notification requirements. (see end note for the full list)[i]

Trade Secret - confidential information that enjoys legal, intellectual property protection.

TRI – Trusted Research & Innovation

UK IPO – The UK Intellectual Property Office, the official UK government body responsible for intellectual property (IP) rights including patents, designs, trade marks and copyright. It is an executive agency sponsored by DSIT.

UKRI – United Kingdom Research & Innovation, the UK's largest single public funder of science and research. It is a non-departmental public body responsible for supporting research

and knowledge exchange, including at higher education institutions, as well as supporting the UK's wider research and innovation system. It includes the research councils, Research England, and Innovate UK, the UK's innovation agency. UKRI is sponsored by DSIT.

Unintentional knowledge leakage - the accidental sharing of confidential knowledge with external parties.

UUK - Universities UK, the trade body for UK universities

[i] The 17 sensitive economic areas are:

1. Advanced Materials
2. Advanced Robotics
3. Artificial Intelligence
4. Civil Nuclear
5. Communications
6. Computing Hardware
7. Critical Suppliers to Government
8. Cryptographic Authentication
9. Data Infrastructure
10. Defence
11. Energy
12. Military and Dual-Use Technologies
13. Quantum Technologies
14. Satellite and Space Technologies
15. Suppliers to the Emergency Services
16. Synthetic Biology
17. Transport

www.ircaucus.ac.uk

Email info@ircaucus.ac.uk Twitter @IRCaucus

Delivered with
ESRC and
Innovate UK