Centre for International
Governance Innovation

CIGI Papers No. 253 — May 2021

Quantifying Trade Secret Theft
Policy Implications

Dan Ciuriak and Maria Ptashkina

Centre for International
Governance Innovation

CIGI Papers No. 253 — May 2021

Quantifying Trade Secret Theft
Policy Implications

Dan Ciuriak and Maria Ptashkina

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Dan Ciuriak is a senior fellow at CIGI, where he is exploring the interface between Canada's domestic innovation and international trade and investment, including the development of better metrics to assess the impact of Canada's trade agreements on innovation outcomes. Based in Ottawa, Dan is the director and principal of Ciuriak Consulting, Inc.

Dan is also a fellow in residence with the C. D. Howe Institute, a distinguished fellow with the Asia Pacific Foundation of Canada and an associate with BKP Economic Advisors GmbH of Munich, Germany. Previously, he had a 31-year career with Canada's civil service, retiring as deputy chief economist at the Department of Foreign Affairs and International Trade (now Global Affairs Canada).

Maria Ptashkina is an economics Ph.D. candidate at University Pompeu Fabra in Barcelona, Spain. Her main research interests include macroeconomics, international economics and trade policy. She is a former fellow at the International Center for Trade and Sustainable Development and former delegate from the Russian Federation to the Asia-Pacific Economic Cooperation Forum. Maria is a former member of intergovernmental policy research groups on issues related to international trade and investment (the Group of Twenty, BRICS [Brazil, Russia, India, China and South Africa] and the One Belt, One Road initiative).

Acronyms and Abbreviations

AI	artificial intelligence
CIPO	Canadian Intellectual Property Office
CSIS	Canadian Security Intelligence Service
DTSA	Defend Trade Secrets Act
EEA	Economic Espionage Act
EUIPO	European Union Intellectual Property Office
IP	intellectual property
KBE	knowledge-based economy
R&D	research and development
STEM	science, technology, engineering and math
TFP	total factor productivity
TRIPS Agreement	Agreement on Trade-Related Aspects of Intellectual Property Rights
TSD	Trade Secrets Directive
UTSA	Uniform Trade Secrets Act
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

Executive Summary

In the modern data-driven economy, trade secrets are becoming a more important part of firms' intellectual property (IP) strategies. For their part, governments worldwide have been introducing new legislation to broaden and toughen the protection for trade secrets, citing estimates of the cost of trade secret theft in the order of one–three percent of the GDP of advanced countries or in the order of hundreds of billions of dollars annually. This paper reviews the rise of trade secrets from relative obscurity to a major issue in international economic governance; analyzes the obligations on firms to establish protected knowledge as a trade secret; considers the evidence on the leakage of trade secrets in terms of frequency, scale and means (for example, cybertheft and intercorporate movements of personnel); and examines the robustness of existing estimates of the value of trade secret theft. Given that IP protection is a two-edged sword, the paper also examines the risks of collateral damage to the vitality of the modern innovation-intensive economy of more expansive protections and harsher criminal sanctions. While the evolution of the economy necessitates modernization of IP protection to address the modern context for trade secret theft, the paper concludes that the available evidence does not support the expansive claims of trade secret theft that have fuelled international tensions and, by extension, points to reform efforts that focus on updating and clarifying trade secrets regimes with a balanced perspective on protecting firms' valuable IP while not undermining the dynamism of innovation systems.

Introduction

Trade secrets as a form of IP is becoming an increasingly important issue in global trade governance. In the modern data-driven economy with its accelerated pace of innovation, trade secrets have become one of the cornerstones of firms' IP strategies, in part because data and the algorithms that exploit data are not patentable or meaningfully protected by copyright, but also because of the relative ease and flexibility of using trade secrets to protect valuable IP in the technologically fluid environment in which firms now function. For their part, governments worldwide have been introducing new legislation to broaden and toughen the protection for trade secrets, including through the IP chapters of trade agreements. And, given alarming estimates of the cost of trade secret theft in the order of one–three percent of the GDP of advanced countries (which would be in the order of $180 billion[1] to $540 billion for the United States alone), trade secrets have become one of the main sources of controversy in the global economy, including serving as one of the main triggers for the trade and technology conflict between the United States and China.

The emergence of trade secrets from relative obscurity to a major issue in international economic governance has taken place over a relatively short period of time and in the context of comparatively limited analysis and debate. Numerous issues bear scrutiny: Is this an across-the-board issue for economies (for example, due to ubiquitous cyber espionage), or is it principally an issue for certain industries or sectors (for example, those whose main capital assets are data and algorithms), or is it about firm-specific shocks (for example, arising at random at a granular level)? How robust are the estimates of the value of trade secret theft that have been routinely cited? By extension, are the forceful countermeasures that have been deployed in the trade and technology domains to counteract trade secret theft commensurate with the scale of the problems, or could these problems be adequately addressed by fine-tuning existing legal protections? And, as is always the case with the two-edged sword of IP protection, what are the risks of collateral damage to the vitality of the modern innovation-intensive economy posed by more expansive protections and harsher criminal sanctions? For policy makers, these are critical questions in framing first-best policy responses. This paper takes up these questions.

For context, until recently, trade secrets did not enjoy statutory protection. Historically, trade secrets entered into common law in England in the early 1800s as a way to protect against the disclosure of proprietary manufacturing knowledge; the treatment of trade secrets subsequently spread internationally and evolved through application of common-law principles (Sandeen and Seaman

[1] All monetary figures in US dollars unless otherwise noted.

2017, 835–36). A coherent framing for trade secrets was in due course established through a restatement of tort law in the United States in 1939, which, while falling short of codification, proved to be highly influential (ibid., 836–37):

- It established liability for disclosure or use of another party's trade secret in breach of confidence or through discovery of the secret "by improper means"; liability extended to third parties aware of the original misappropriation.
- It required that the trade secret be, in fact, secret so that it would require improper means to obtain.
- It limited protection to trade secrets that were actually in commercial use.
- It provided a definition of potential trade secrets as consisting of "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."
- It provided for a range of remedies, including injunctive relief, damages for past harm and disgorgement of the defendant's profits.

The United States passed its first trade secrets legislation only in 1980, at the beginning of the knowledge-based economy (KBE) era.

Commensurate with its low profile, the topic received rather limited scholarly attention. Perhaps the most significant practical issues debated were: how to deal with the leakage of knowledge that key employees took with them when changing firms (von Kalinowski 1961); whether trade secrets should be treated as conventional property rights (for example, by offering protections under trade secret law against reverse-engineering); and, more fundamentally, why the law offered protection for trade secrets as such in the first place, when another instrument — the patent — was available (Friedman, Landes and Posner 1991).

As the KBE transitioned into the data-driven economy, things started to change. With the rise in the value of data and algorithms for artificial intelligence (AI) as part of corporate intangible assets, there has been a steep growth in reliance on trade secrets as part of corporate IP strategies (Wajsman and García-Valero 2017), including as a substitute for patents (Png 2017). As Richard Kemp (2020) notes: "In a legal environment where attaching IP rights to data is challenging, trade secrecy is therefore emerging as the most likely candidate right, especially in a more digitally connected, AI- and cloud-enabled world." Moreover, as IP has generally grown in importance in business strategies, firms have found trade secrets an increasingly attractive tool on a practical level. This reflects the fact that trade secrets cover virtually any type of commercially valuable information, are indefinite in duration, are flexible in that they do not require modification to cover incremental innovations, and can be invoked by what have been described as "do-it-yourself" approaches — contracts and internal security measures (Linton 2016).

Not surprisingly, as firms came to increasingly rely on trade secrets, there has been a commensurate increase in resort to litigation to protect them (Almeling 2012).

Reflecting the increased importance of trade secrets in firms' IP strategies, the European Union adopted in 2016 a directive to protect undisclosed know-how and business information, which it described as "the currency of the knowledge economy."[2] Similarly, the United States passed into law the Defend Trade Secrets Act of 2016 (DTSA).[3] In both cases, the new laws provided an updated and unified trade secrets regime supplementing various state-level regimes in the respective jurisdictions. Japan and China also upgraded their trade secrets protection laws in 2016 and 2018, respectively (O'Connell 2019).

What really brought trade secrets into the policy spotlight, however, was the prominent role of allegations of trade secret theft in the US trade and technology war against China. In its negotiations toward a trade agreement, the US side demanded that China better protect American IP and stop forced technology transfers, cyber theft and trade secret misappropriation, among other things (see, for example, Lester and Zhu 2020). Many of the US trade measures against China, such as the section 301 tariffs, were justified on trade secrets theft grounds: as the United States stated in its submission

[2] *Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, [2016] OJ, L 157.

[3] *Defend Trade Secrets Act of 2016*, S. 1890, 114th Cong, § 2 (2016).

to the World Trade Organization (WTO) in the case brought by China against these measures, "China's acts, policies, and practices addressed in the relevant Section 301 Report amount to 'state-sanctioned theft and misappropriation of U.S. technology, intellectual property, and commercial secrets'" (WTO 2020, para. 7.100).

As for the scale of trade secret theft, this has been placed as high as between $180 billion and $540 billion annually for the United States alone by the Commission on the Theft of American Intellectual Property (Blair and Huntsman, Jr. 2017, 11). These estimates, however, have been called into serious question. Methodologically, they depend on a 2014 study (Michel, Stronberg and Geday 2014) that generates an estimate of the value of trade secret theft based on statistical guesstimates of the scale of various other illegal activities, such as narcotics trafficking, corruption, occupational fraud and illicit financial flows, rather than, for example, building up an estimate from actual evidence of cases of theft. As observed by Stephen Roach (2019), "it takes a rather large leap of faith to convert this information into the 1–3 percent of GDP that the IP Commission claims is lost to theft of intellectual property."

The foregoing observations establish that the protection of trade secrets is an increasingly important issue for economic governance in the modern data-driven economy. In particular, given the large and growing role of trade secrets as a legal instrument of choice in corporate strategies to protect corporations' valuable IP, there are grounds for updating legal protections for companies relying on trade secrets laws, including through international agreements and enforcement mechanisms. At the same time, the widely cited estimates of the costs of trade secret theft as being in the order of one–three percent of GDP have been called into question, and there are significant gaps in the literature on the impacts of trade secret protection on innovation, trade and investment (Linton 2016).

This paper seeks to provide insights for policy makers into the open questions in this area: the extent to which trade secrets protections need to be strengthened as opposed to simply modernized, and whether there is any support for the much more serious charges concerning large-scale leakage of technology via trade secret theft that have been made to support the trade and technology war.

The paper is organized as follows. It first sets out the current policy setting for the treatment of trade secrets. It then considers the empirical evidence on trade secret theft, including the channels through which such theft typically occurs, and what this means for international leakages of technology. Against this background, the paper critiques the current approach to quantifying trade secrets theft on first principles grounds by considering international trade secret theft as a form of cross-border disembodied technology flow. The paper further considers how such flows might properly be evaluated and how these values compare to the totality of cross-border technology flows. The conclusion discusses the implications for policy.

Background

Some Trade Secret Basics

Trade secrets, which, in law, may also include undisclosed — or confidential — information, constitute the fourth leg of the IP stool, alongside patents, trademarks and copyright (see, for example, Pooley 2013). Trade secrets are an important resource for companies whose intangible assets are not patentable but have commercial value. Trade secrets may come in different forms, including a formula, pattern, compilation, program, device, method, technique, process or algorithm. Some of the best-known examples of trade secrets are Coca-Cola's recipe, the KFC coating recipe and Google's internet search algorithm. Notably, a trade secret can involve "negative" information — knowledge about "research blind alleys, failed designs, and methods that do not work" (Saunders and Golden 2018, 72).

To qualify as a trade secret, the information in question must generally meet three criteria: it must have either actual or potential independent economic value by virtue of not being generally known; it must have value to others who cannot legitimately obtain the information; and it must be subject to reasonable efforts to maintain its secrecy (United States Patent and Trademark Office 2020). If any of the three criteria ceases to be met, the trade secret ceases to exist. Unlike protection for patents and copyrights, trade secret protection is not limited in term.

As for the scope of what is understood to be covered as a trade secret, language varies. For example, article 39(2)(a) of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) elaborates on the meaning of "generally known" by specifying that the information must be "secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question."

Language also varies with regard to the strength of measures to protect a trade secret. For example, the Canadian Intellectual Property Office (CIPO) states that a business must "take all possible measures to ensure that the business information remains a secret" (CIPO 2021). Meanwhile, the World Intellectual Property Organization (WIPO) (2020) elaborates that the "reasonable steps" or measures "taken by the rightful holder of the information" include "the use of confidentiality agreements for business partners and employees." Ioana Vasiu and Lucian Vasiu (2017) comment on the meaning of "reasonable measures": "The 'reasonable' security measures requirement can be understood as 'not excessive or extreme,' 'moderate, especially in price,' without the need to employ every conceivable type of measures."

Shreya Desai (2018), meanwhile, provides a description of the elaborate lengths that Coca-Cola goes to protect its famous trade secret recipe: "This recipe sits in a vault in Atlanta, Georgia with a palm scanner, numerical code, and large steel door. Once inside the vault, there is another safe box and metal case that store what the owners call 'the most guarded trade secret in the world.' Only two senior executives know the recipe at any given time, and they are not allowed to travel on the same plane" (references in the original omitted).

What stands out here is that the level of measures taken to protect a trade secret likely scales with the value of the trade secret. Ordinary measures might be deemed sufficient for trade secrets of moderate value; by the same token, most trade secret theft is likely to involve information protected by ordinary measures, which is to say, secrets of only moderate value.

An important distinction is that between trade secrets and tacit knowledge, or general skills and knowledge that employees acquire in the course of their job tenure. To the extent that maintaining exclusive access to such skills and knowledge is crucial for a company's commercial success, it is the responsibility of the employer to take measures to protect this knowledge, for example, through non-disclosure or non-compete clauses in employment agreements. At the same time, given the public interest in keeping the labour market flexible and liquid, such clauses may be subject in some jurisdictions to meeting a test of being both reasonable and in the public interest (Courage and Calzavara 2015). In their review of courts' practice, Kurt M. Saunders and Nina Golden (2018, 99) find that having a non-disclosure or non-competition agreement was not an indicator that courts would necessarily find the existence of a trade secret. In fact, courts have more often found a trade secret to exist in cases lacking some type of employment agreement than in those that had such an agreement. In short, there is no bright line distinguishing a trade secret belonging to an employer from the human capital of the employee.

As for what constitutes theft, US federal law addresses cases where misappropriation of information is "related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret" (United States Patent and Trademark Office 2020). Loss of value to the holder of the trade secret is essential for there to be an offence — and loss of value to the owner of the secret implies the ability to bring on to the market a competing product. Accordingly, the context matters in determining whether a breach of information security amounts to trade secret theft or not.

In the event a case of trade secret theft has been proven, courts can order the party that misappropriated the trade secret to maintain its secrecy, pay a royalty to the owner or pay damages.

In legal proceedings, if the owner of the trade secret is found to have failed to maintain its secrecy, if parallel discovery or reverse-engineering is established, or if any other independent disclosure of information occurs, protection for the trade secret is lost (see Saunders and Golden 2018, 75).

These issues were recently highlighted in a case brought by the US Federal Bureau of Investigation against a visiting Chinese scientist at the University of Virginia who had been arrested on allegations of stealing trade secrets; the case was dropped after the university acknowledged the scientist was authorized to access some of the material (O'Keeffe and Viswanatha 2020).

Similarly, in a case tried in 2018, *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, the decision went against the plaintiff, Yellowfin, on the grounds that its measures to protect the information at issue were inadequate (see Grimes and Murphy 2018). Yellowfin's measures included limiting access to the information to less than five percent of employees in the company, maintaining the information on a password-protected computer system and giving verbal admonishments not to share the information with third parties. However, the information had not been marked as confidential and the defendant:

→ had been encouraged to store the information on a personal laptop and phone;

→ had not been instructed to secure the information on his personal devices;

→ had not been required to delete the information from those personal devices when he left the company; and

→ had been allowed access to the information even though he had refused to sign a confidentiality agreement.

These considerations underscore the lack of clarity concerning adequacy and fitness for purpose of security measures in any given situation, given the nature of the secrets being protected and the technological environment. They also underscore the potential for a gap to exist between perceptions of trade secret theft and the legal reality.

The Rise of Trade Secrets as IP Strategy

The rise of the importance of trade secrets is endogenous to the changing nature of the economy and technology. Three developments in particular have driven matters.

First, the rapid expansion of the digital economy has generated a steeply growing stock of intangible assets that are more easily protected by trade secret laws than by other forms of IP protection. These intangible assets include software, algorithms, cloud-based solutions and, above all, data.

Second, reforms to IP policy in the leading IP jurisdictions have upgraded trade secret laws while at the same time making patent laws less accommodating to rights holders. This has prompted a relative increase in trade secrets case filings. For example, according to a report by Lex Machina (2018), trade secret case filings in US federal district courts were steady at around 900 cases per year until 2017; filings then increased sharply by more than 30 percent over the previous year. The report attributes this increase to the passing of the DTSA (discussed further below). In addition, increased attention to trade secrets from tax authorities is also likely raising awareness. For example, the Organisation for Economic Co-operation and Development base erosion and profit sharing guidelines and the EU Anti-Tax Avoidance Directive mention trade secrets as intangible assets that require proper management (O'Connell 2019).

Finally, increased information diffusion raises the risk of trade secret leakage, while at the same time compromising reliance on trade secrets as a way to protect information. With the rise of the open innovation paradigm (for example, through increased collaboration between universities, suppliers and vendors, content providers and end-users), valuable information is shared with a number of different parties, breaking the secrecy or creating a shared ownership. In addition, the shift in employment patterns toward higher labour mobility (as opposed to traditional indefinite contracts) increases the flow of tacit knowledge between companies and simultaneously drives increasing use of non-disclosure agreements and restrictions on post-severance employment to protect trade secrets.

The Evolving Legal Regime for Trade Secrets

All members of the WTO, as parties to the TRIPS Agreement, are obliged to provide trade secret protection. In particular, article 39(2) requires members to provide means for protecting information that is secret, commercially valuable because it is secret and subject to reasonable steps to keep it secret. Thus, all WTO members should have the relevant legislation in place. Since the TRIPS Agreement came into force, trade secret law has developed, generally, in a pro-rights-holders' direction.

In the United States, which has led the move to increase protection for trade secrets, trade secret theft has been subject to federal criminal penalty since the passage of the Economic Espionage Act (EEA) of 1996. Meanwhile, private actions to obtain civil remedies for trade secret misappropriation could be pursued at the state level, either under common law or under a particular state's implementation of the Uniform Trade Secrets Act (UTSA) published in 1979 and amended in 1985 (Pooley 2016). Some version of the UTSA has been enacted in 48 states. The federal DTSA is similar to the UTSA in providing for injunctive relief, compensatory damages, exemplary damages and the recovery of attorneys' fees. The new legislature, however, facilitates pursuit of remedies for alleged trade secret theft in several ways:

- It allows plaintiffs to file trade secret theft complaints in federal courts; previously, redress could be sought in federal courts only under special circumstances (United States Patent and Trademark Office 2020).
- It provides for *ex parte* seizure of goods allegedly produced via misappropriated trade secrets and of objects such as laptops, flash drives and paper documents that allegedly contain misappropriated trade secrets. This provision relieves the trade secret owner of the costs associated with the discovery process of a lawsuit and shifts these costs to the public.
- It extends the statute of limitations period from three to five years.
- It provides for treble exemplary damages, compared to double under the UTSA.

There was strong support for the DTSA from big businesses, but also concerted opposition from the legal profession (Pooley 2016, 1046). Many of the concerns about the DTSA are based on the following considerations:

- the impact on the domestic economy (an *ex parte* seizure can effectively shut down a competitor without any litigation, hence opening up the legislation to anti-competitive abuse) (Liebesman 2017);
- due process grounds (a judge would be required to decide a fact-intensive case with only one side of the story, when possession of a trade secret through reverse-engineering, for example, is quite legal) (Levandoski 2018); and
- potential impairment of domestic labour mobility (employees, who are the most common defendants in trade secret cases, are left uncertain about exposure to trade secret liability, given the opportunity for forum shopping created by the failure of the DTSA to pre-empt state law, and thus might be discouraged from changing employment (Bruns 2017).

Clearly, these same concerns would also extend to the international domain, especially in the currently charged political context.

Other notable actions to expand and strengthen trade secrets protection in the United States include an amendment to the EEA that increased the scope of trade secrets protection. This legislative reform directly responded to the decision in *United States v. Aleynikov*, which overturned the jury verdict finding that the defendant stole a computer code from his employer. The court overturned the initial decision because the computer code failed to satisfy the requirement that a "product" was "produced for" or "placed in" interstate or foreign commerce. The amended legislation now applies to a trade secret "that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof." As well, the EEA was updated in 2012 to increase penalties for certain violations of the act: the upper limit of penalties for offences by individuals was increased from $500,000 to $5 million, and the upper limit for the offences by corporations was increased to $10 million, or three times the value of the stolen trade secret.

EU trade secrets law has also evolved, generally in the direction of increasing protection, but also introducing some disciplines. In 2016, EU law was harmonized through Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive [TSD]). The TSD set a minimum level of protection that each state must implement, including provision for injunctions and corrective measures, with a deadline for implementation of June 2018. As for how the TSD regime compares to US levels of protection, it has been argued that the TSD will do for the European Union only what the UTSA did for the United States, but leave the European Union short of where the United States is with the DTSA (Desai 2018).

A report commissioned by the European Union Intellectual Property Office (EUIPO) (2018) Observatory on Infringements of Intellectual Property Rights assessed the legal system of EU member states with regard to trade secret protection pre-TSD implementation as being extremely heterogeneous, with no unified definition of what constitutes a trade secret, varying scope of protection and different sources of law. The TSD sets out to remedy these issues. First, it established a uniform definition of a trade secret as being any information that has commercial value because it is secret (in the sense that it is not generally known among or readily accessible to persons within the relevant circles of trade), including negative information. This broadens the scope of some definitions previously used in the member states. Second, it established the requirement for trade secrets to be subject to reasonable protection measures. Previously, in some countries, such as Germany, the mere intent of the trade secret owner to keep the information secret was sufficient. The TSD states that companies must actively take reasonable action to protect their trade secrets (for example, through non-disclosure agreements or non-compete clauses).

At the same time, the TSD strengthens the position of employees, including by ensuring their freedom to take with them any knowledge and experience gained during their tenure on to their next employer. The confidentiality of valuable information thus becomes the responsibility of the employer to protect.

Moreover, the TSD generally allows reverse-engineering; in Germany's previous legislation, for example, reverse-engineering was only allowed in certain situations. This limits the use of time-unlimited trade secrets and creates incentives to use patents, which have the advantage from a public policy perspective of publication of the information with longer-term enhancement of competition.

Other countries have also had notable changes to their trade secret regulation over the past few years. Japan's Unfair Competition Prevention Act had a major update on January 1, 2016, following a series of incremental changes since 2003. In 2019, a new version of the act came into effect; this is said to be the first law in the world to protect big data itself (Sagara 2019). China's Anti-Unfair Competition Law was updated on January 1, 2018, and then again on April 23, 2019. The latest amendment broadens the definition of a trade secret, adds new types of trade secret infringements (in particular "cyber invasion"), expands the scope of persons who are subject to the provisions of trade secret infringement to include all individuals and entities, increases penalties for trade secret infringement and adds a new article concerning the burden of proof in trade secret lawsuits (Zhang 2019).

Empirical Evidence on Trade Secret Theft

Empirical evidence on the value of trade secrets theft on an annual basis is thin, to say the least. One reason is that "secrecy disputes are usually secret, so they do not become part of the public debate" (Pooley 2013). This section examines such systematic evidence as there is, anecdotal evidence and inferred estimates.

Awards in Litigated Cases

Systematic evidence based on damages awarded pursuant to legal suits suggests annual totals are comparatively modest, notwithstanding the rising number of cases. Stout, a global advisory firm, has compiled data on the results of trade secret litigation covering the three-decade period from 1990 to 2019. Plaintiffs received favourable decisions in 68 percent of the cases (Mordaunt, Eisgruber and Swedlow 2020, 9); monetary damages were awarded in 52 percent of the cases, with the total amount (inclusive of compensatory and punitive damages and attorney fees) amounting to about $3 billion, or approximately $100 million per year (ibid., 10).

In terms of the number of cases, about 1,100 federal cases were filed between 2010 and 2015; the pace rose to about 1,400 cases since the passage of the DTSA (ibid., 13). Accordingly, given that damages were awarded in more than half the cases, most awards were very small. Only five cases are reported as having exceeded $100 million, one of which was the high-profile Uber-Waymo case, which resulted in a settlement of $245 million (ibid., 14).

Lex Machina (2018) also has compiled aggregate data on trade secret damages awarded in the United States under state and federal legislation from 2009 to the second quarter of 2018. The reported total amounted to about $1.72 billion, or around $172 million annually (ibid.). Modest as these figures are, the figures appear to be even more so upon closer examination. For example, of the $1.72 billion in awards over the period 2009–2018, $920 million, or about 50 percent of the total, was in one award granted by a jury in 2011 that was later vacated on appeal in 2014 (ibid., 10). This case was eventually settled in 2015 with a payment of $275 million in restitution; the defendant (a Korean firm) also paid $85 million in criminal fines (United States Department of Justice 2015). Taking this adjustment into account reduces the annual figure to the ballpark of the Stout report (Mordaunt, Eisgruber and Swedlow 2020).

Some highlights from the 2020 Lex Machina report are as follows:

- In 2019, US courts awarded damages in fewer trade secret cases than in 2018 but a larger amount of money was awarded overall — $105 million in 2019 versus $71.9 million in 2018.
- In 2019, the top filer was DiscoverOrg, a Vancouver, Washington-based business database that brought 19 cases in 2018 against people allegedly accessing its data without authorization.
- Of terminated cases, 156 ended for failure to identify a trade secret; 116 were terminated for failure to maintain secrecy.
- The top plaintiff over this period, with 51 cases filed, was not a high-technology company but rather the insurance firm Allstate Corporation (Reisinger 2020).

Overall, the value of trade secret theft as reflected in court restitution awards is relatively modest. The average flow of damage awards is in the order of $100 million per year. The awards are highly skewed, with only a handful of relatively large ($100 million or more) awards and a large number of very small awards. While the reports do not break down the awards on the basis of nationality, a major part of the awards are likely to be intranational — that is, US firms paying damages to other US firms. This would be consistent with interfirm employee mobility being the most important source of trade secret misappropriation (for example, the move of Anthony Levandowski from the employ of Google to Uber, which was the source of the trade secret theft case between Uber and Waymo; Statt 2020). This follows from the fact that most interfirm movement of personnel is within a country as opposed to between countries.

Anecdotal Evidence

The prominence of trade secret theft as a public policy issue is closely linked with the rise of allegations of IP theft by China. In the absence of systematic evidence, the case against China is based on anecdotal evidence. The sense of large values comes mainly from the claims made by plaintiffs. However, cases often wind up dismissed, modified and/or result in awards that are a small fraction of the original claims — if any award is made at all. Accordingly, it is important to look for the final settlements, which often take years to reach.

For example, a case brought against two scientists at Eli Lilly involved alleged theft of trade secrets worth $65 million. The charges were first watered down to "wire fraud" and then dismissed entirely (although the individuals falsely accused suffered enormous personal damage with reputations attacked and one having been incarcerated for the better part of a year on grounds of being a flight risk; Silverman 2014). Similarly, US federal prosecutors dropped all charges against a Chinese American scientist, the chair of Temple University's physics department, who had been accused of sharing sensitive American-made technology with China; as it turned out, prosecutors had misunderstood the science (Thomas 2016). In the prominent ongoing case of alleged theft of IP from GlaxoSmithKline, the US government valued the information in question in excess of $550 million while acknowledging "this amount may be contested" (D'Annunzio 2020).

No company has figured more prominently in the US case against China for IP theft than Chinese telecommunications equipment provider Huawei. As Chuin-Wei Yap et al. (2019) write: "Theft and industrial espionage are relatively common in the global tech industry, and Huawei isn't the sole company to face accusations of stealing foreign IP. What set Huawei apart, its accusers say, was the flagrancy of its plagiarism."

Huawei has been involved in 10 US federal court cases (ibid.). Of these, the ones most frequently mentioned (in fact, the only ones the authors found mentioned in the public discourse) are the following:

- In December 2017, Huawei brought a trade secret case against San Jose, California-based CNEX and a former employee, Yiren Huang, who helped start CNEX in 2013 — three days after leaving Huawei. Huawei sought $85.7 million in damages and rights to CNEX's memory-control technology (McWilliams 2019). In a counterclaim, CNEX argued that a circuit board provided to a visiting Chinese scholar for a research project had been inappropriately used for a study tied to Huawei. The case was settled in June 2019, with the jury finding fault on both sides. However, no awards were granted on grounds of no damage having been suffered (Freifeld 2019). As for the financial aspects, CNEX General Counsel Matthew Gloss stated: "This is a victory for the rule of law and for global standards of ethical corporate behavior....This case was never about money" (McWilliams 2019).

- Quintel Technologies sued Huawei in 2015 for theft of antenna technology. The lawsuit was settled in 2018 without apparent monetary damages awarded; in particular, the "unjust enrichment" claim against Huawei was dismissed (Leagle 2018).

- In the high-profile indictment of Huawei issued by the US Attorney General in 2019 for alleged trade secret theft (United States Department of Justice 2019), the specific instance cited was several years old (dating back to 2012–2014) and had already been settled in a civil suit with damages amounting to $4.8 million. The main cost alleged by the complainant (T-Mobile) was that of switching cellphone suppliers rather than the value of the alleged trade secrets stolen (Lerman 2017); the court awarded no compensation for trade secret loss in this instance. Of interest in this case is the argument advanced by Moshe Adler (2019) that "the problem was not that [Huawei] did not understand how Tappy [a robot device that tapped cellphones to test them] works [and wanted to steal it], the problem was that Tappy did not work and that T-Mobile was reluctant to acknowledge it." As noted, negative trade secrets are still trade secrets; however, the moral opprobrium is somewhat mitigated.

- Previously, in 2010, Huawei and Motorola Solutions (a Motorola spinoff) settled a pair of lawsuits, with Motorola Solutions alleging Huawei conspired with former employees to steal trade secrets and Huawei blocking a sale by Motorola Solutions on the basis that it included Huawei technology. Motorola Solutions made a monetary payment to Huawei to settle the suits (Barboza 2011).

- A still earlier case (described as "infamous" in a 2019 *Foreign Policy* article by Keith Johnson and Elias Groll 2019) involved a Cisco claim brought against Huawei for copying certain lines of source code used in routers and switches plus copyright violations in using extensive parts of its user documentation verbatim. As Yap et al. (2019) elaborate, the copying was so extensive that Huawei inadvertently copied Cisco typos in its manuals and could not release its routers for shipment until it fixed a substantial number of the common Cisco bugs it had copied, for fear of giving away its plagiarism. Cisco Systems dropped the suit after Huawei removed the offending Cisco IP from its products. According to Huawei's press release, the US court dismissed Cisco's claim with prejudice (i.e., disallowing further litigation) following the end of a third-party review process. Each party covered its own costs (Leyden 2004).

Whatever one might wish to make of the cases that went to court and were tried, they hardly inspire confidence that there is an abundance of evidence to support claims of steeply growing, high-value trade secret cross-border theft worth in the order of hundreds of billions of dollars annually.

The main story circulating on Huawei's alleged trade secret theft concerns Canada's Nortel Networks. Conrad Black (2019), for example, bluntly states "the almost certain fact that Huawei's business was largely built on one of the most colossal and protracted thefts of information and violations of patent laws in the lengthy history of industrial espionage, chiefly at the expense of this country [Canada]." The supporting case builds on various stories:

- At the 2004 Chicago Supercomm conference, a Huawei employee (subsequently fired) was detained by security personnel for opening networking equipment to photograph the circuit boards. Confiscated materials included "memory sticks with the photos, a notebook with diagrams and data belonging to AT&T Corp., and a list of six companies including Fujitsu Network Communications Inc. and Nortel Networks Corp" (Yap et al. 2019).

- According to an ex-Nortel employee, the company's email system was hacked by accounts traced by the employee back to China (according to Black [2019], the breach was discovered in 2004). Nortel's executives were, however, "mostly disinterested in the investigation and did little more than change executive account passwords" (Cooper 2020).

- In addition to the internal warnings, the Canadian Security Intelligence Service (CSIS) warned Nortel of possible spying by China (Blackwell 2020).

- A listening device was found in Nortel's former offices when CSIS moved in, in 2009.

- After Nortel collapsed, Huawei hired some of its engineers: "On a wall of fame for stars of the Chinese company were several former employees of Nortel, the Canadian telecommunications giant that suffered a spectacular collapse" (ibid.).

- Former Nortel security personnel report that "a customer tied to Huawei returned a piece of equipment that had been pulled apart and 'reverse engineered' to divine its secrets" (ibid.).

Telecommunications is a backbone infrastructure service that has historically been subject to foreign investment restrictions because of national security concerns. Cybersecurity was definitely on the radar of governments; indeed, the White House published its *National Strategy to Secure Cyberspace* in February 2003 (Fischer 2005). Nortel received a security briefing on espionage from Canada's national security agency. And Nortel had mounted court cases against US firms it claimed were trying to steal its trade secrets (CBC News 1999). If indeed the "crown jewels" of Nortel's IP cache were accessed by hacking email accounts, that would amount to extraordinary negligence since, from a formal trade secret theft perspective, a failure to secure the trade secrets means the trade secret does not exist. Meanwhile, reverse-engineering and hiring former staff from competitors are legal.

Nortel's IP strategy appears to have been focused on patents: its patent holdings were auctioned off for $4.5 billion (Bagnall 2011). That it had trade secrets is clear from its litigation history. How important they were to its overall business is simply not clear. Informal opinions such as Black's place the fault for Nortel's failure in Canadian naiveté; formal analysis such as that of Gregory Richards et al. (2014) attributes it to management failure. In the court of Canadian public opinion, of course, none of this stands to reverse the opinion that what is currently Huawei's should have been Nortel's. But the smoking gun of trade secret theft as the cause of Nortel's demise is hard to find. And it must be emphasized that this is the alleged trade secret theft of the century.

Inferred Estimates

The most influential assessment of the value of trade secret theft is that developed by Marissa Michel, Craig Stronberg and Peter Geday (2014), who estimate the annual amount of trade secret theft to be in the order of one–three percent of the GDP of advanced industrialized nations. On the basis of these estimates, the *IP Commission Report* assesses that the losses to the American economy are in the order of $180 billion to $540 billion per year (Blair and Huntsman, Jr. 2017). This study and figures derived from this study are commonly cited in the literature (for example, see Vasiu and Vasiu 2017, 7). The Office of the Director of National Intelligence, meanwhile, suggests that "economic espionage through hacking costs the U.S. economy $400 billion a year" (cited in Blair and Huntsman, Jr. 2017, note 13); much of this would also be due to trade secret theft, presumably.

The economic meaning of these figures is not explicitly stated by Dennis C. Blair and Jon M. Huntsman, Jr. (ibid.); however, from the context, it appears to be equivalent to lost sales by US firms. For example, in commenting on the losses to the US economy from counterfeit goods — with which the trade secret theft figures are rolled up — this report states: "The Commission believes that these goods did not displace the sale of legitimate goods on a dollar-for-dollar basis and estimates that at least 20% of the total amount of counterfeit and pirated tangible goods actually displaced legitimate sales. Thus, the cost to the American economy, on the low end of the estimate, is $29 billion."

Another report from the same period by McAfee and the Center for Strategic and International Studies (2014) estimated the global cost of cybercrime to be between $375 billion and $575 billion. This study covers not only IP and confidential business information theft but also financial crime, recovery costs for data breaches and economic losses due to impaired incentives to invest in innovation. At the same time, it does not cover the most important avenue for trade secret leakage, which is the movement of personnel between companies. While the figures from this study do not, accordingly, bear directly on the question addressed in the present study, the role attributed to IP and confidential business information theft is large and hence this study supports the conclusion that the value of trade secret theft is in the hundreds of billions of dollars annually.

Another relevant report (PricewaterhouseCoopers 2018) was commissioned by the European Commission on the costs of cyber espionage. This report mentions the McAfee and Center for Strategic and International Studies (2014) study results to support an estimated cost of cyber espionage in the hundreds of billions of euros. It also mentions a report by Hosuk Lee-Makiyama (2018), which concludes that cybertheft results in up to €60 billion in foregone economic growth for the European Union and 289,000 jobs.

The latter report relies heavily on an original study of the transfer of knowledge via espionage from East to West Germany. This study documents a significant narrowing of sectoral total factor productivity (TFP) as a result of East Germany's industrial espionage: specifically, the average TFP gap between West and East Germany at the end of the Cold War would have been 6.3 percentage points larger had East Germany not engaged in industrial espionage (Glitz and Meyersson 2017). This represents an incremental annual income gain of 0.3 percent for East Germany.

From a narrowly legalistic trade secret perspective, given the general restrictions on trade that prevailed during the Cold War and hence the limited economic competition between East and West Germany, it may be concluded that these knowledge flows to East Germany enhanced living standards in East Germany at little, if any, cost to West Germany. Accordingly, these knowledge flows may not even have qualified as trade secret theft (which requires loss to the owner of the trade secret). Be that as it may, for the time being, the central point is that there is some evidence for economically meaningful flows of technology via espionage.

If this implied annual income gain of 0.3 percent could be applied to global GDP, it would suggest a gain of about $278 billion in 2019 (given global GDP of $86.6 trillion; International Monetary Fund 2019). However, this estimate would be clearly inappropriate, since it would not apply to knowledge transfers between the leading technological societies (i.e., between the United States and the European Union, for example), which operate at the same technological level (unlike the case with East and West Germany). Moreover, it would not apply to the least developed countries that lack the technological sophistication to go fishing for trade secrets, which East Germany did have, given its legacy of German industrial knowledge. Indeed, the circumstances in which it would apply would be quite rare: two societies with comparable capacity to absorb new technology but operating under sufficiently different technological circumstances to make commercial espionage worthwhile. This is a fair description of the East-West German dyad; however, it is not a fair description of most of the world. In short, this study provides evidence that technology does flow across borders through economic espionage and also sets a ceiling on the likely value of these flows because of the unusually conducive circumstances for such transfer in the two economies studied.

Trade Secrets: The Proxy Methodology

The above discussion underscores the problems with the available evidence on the scale of trade secret theft. Systematic evidence on the value of trade secret theft for an advanced economy based on legal settlements puts the value of annual theft in the order of 0.0005 percent of US GDP (about $100 million on a 2020 GDP of about $20 trillion in the United States). If we assume that one-third of US earnings on licensed IP comes from abroad, this would scale the foreign share of trade secret theft at about one-third of this figure, or about $33 million, which is vanishingly small as a share of GDP. Anecdotal evidence is inadequate to overturn this conclusion. By contrast, the proxy methodology that is heavily relied upon suggests the true figure is much higher at about one–three percent of GDP. This section considers the robustness of the proxy methodology.

The Proxy Methodology

The proxy methodology is based on the premise that the losses from trade secret theft, measured in terms of lost sales by firms, are on the scale of other illicit activities, such as occupational fraud, tax evasion, corruption, copyright infringement and software piracy, narcotics trafficking, black market activities and illicit financial flows. As per the survey conducted by Michel, Stronberg and Geday (2014), available evidence on these various illicit activities places the costs to the economy at a small fraction of the value of licit activities, with the authors settling for a range of one–three percent as most reasonable.

As a first step, Michel, Stronberg and Geday (ibid.) observe that research and development (R&D) expenditures in the United States amount to about 2.5 percent of GDP; at the global level, the ratio of R&D to GDP is about 1.8 percent (ibid., 8). This figure is used to establish a lower bound for the value of trade secrets since it is argued that "the value of trade secrets in the marketplace represents a significantly greater component of GDP than illustrated by R&D spending alone."

The problems with this quantification are perhaps too many to enumerate. Suffice it to say that the main connection between R&D and IP in the economic literature runs through patents, not trade secrets (see, for example, Griliches 1984). Today, the world's most innovative firms in sectors ranging from pharmaceuticals to semiconductors to software are also leading patentors (Columbus 2019). Alongside the rise in the amount of IP accounted for by trade secrets, patent applications filed worldwide have also risen steeply, more than doubling to 3.3 million in 2018 from the amount filed in 2004 (WIPO 2019, 12). Further, much of the value of trade secrets in today's data-driven economy lies in the market valuation placed on the data amassed by companies and the algorithms that have been developed to exploit this data. Most of this value is not connected with R&D activity; rather, it is connected with market activity that generates data (such as internet activity by Google and Facebook users).

A further concern with using the R&D share of GDP (1.8 percent of global GDP) as a core proxy to support a value of trade secret theft in the order of one–three percent of GDP rests on the implausible assumption that more trade secrets are stolen than are developed by companies in any year. Recalling the requirement for firms to take measures to protect trade secrets from the risk of the information losing the standing of a trade secret, this line of reasoning starts at a dead end rather than arriving at one.

Turning to the proxies for the value of illicit activity, Michel, Stronberg and Geday (2014) make the claim that there are "similarities between trade secret theft and other forms of illicit activity." However, the only apparent "similarity" between trade secret theft and the forms of illicit activity identified is, in fact, illegality. There is no evidence or argument presented in the study to actually calibrate characteristics such as the frequency and scale of individual events, or to draw out similarities between the commercial consequences of illicit actions within these other areas of criminal activity and the commercial consequences of trade secret theft. Further, the estimates of the costs of other types of illegal activities are themselves highly imprecise. Moreover, they are drawn from different studies and thus are not aligned across time periods and country groupings. Finally, out of all eight listed proxies, a subset of four indicators that lies between one and three percent of GDP is arbitrarily chosen to support the conclusion that trade secret theft must fall within the given range.

A simple back-of-the-envelope counterfactual calculation suggests that, if the lower bound estimate of the Michel, Stronberg and Geday (ibid.) study were a realistic valuation of the true scale of actual trade secret theft ($180 billion), then actual awards amount to only 0.056 percent of actual costs. The number drops to 0.019 percent when imagining that the upper bound estimate ($540 billion) is true. Given that companies are commercial enterprises seeking profits and market shares, it is hard to imagine firms adopting behaviour (recall the measures adopted by Coca-Cola) that would allow 99.95 percent of all trade theft to pass without legal action, notwithstanding that they must have spent considerable resources to protect these secrets in the first place in order for the information protected to have the status of a trade secret.

A More Realistic Proxy

A more realistic proxy for trade secret theft is “shrinkage,” or loss of goods by retailers through shoplifting, employee theft and supplier fraud. The rationale is as follows:

→ First, both are cases of theft, which have to involve instances of opportunity, motive and means.

→ Second, companies take active measures to protect their merchandise from theft, commensurate with the value of the objects; the same is true of trade secrets.

Accordingly, there are important similarities between the two kinds of theft in terms of the “arms race” between value of property that can be stolen and the effort expended to thwart that theft.[4]

Estimates of shrinkage are readily available. For example, in US retail, the average shrinkage percentage in 2019 was reported at 1.62 percent of total inventory (National Retail Federation 2020). This includes shoplifting, employee theft, vendor malfeasance and other illegal activities. The percentage is within the range found by Michel, Stronberg and Geday (2014); however, the retail shrinkage estimate is much more robust for the purposes.

As for measures taken by retailers to limit shrinkage, these include video surveillance, point-of-sale fingerprinting, burglar alarm systems and so forth. Companies guard trade secrets with similar technological measures (again, recall the Coca-Cola measures).

Further, similarities between shrinkage and trade secret theft include the multiple channels and, in particular, the role of employees (in the case of trade secret theft, the role of employees moving on to new jobs or starting up new companies).

The key issue is to identify the legal commercial flow, of which trade secret theft would be a small fraction. For shrinkage, that underlying commercial flow is total inventory. Given that trade secret theft is being treated as a cross-border problem, the question arises as to what is a cross-border flow that is analogous to the flow that is subject to shrinkage.

The theft of a trade secret amounts to a disembodied technology flow. Legal disembodied technology outflows for the United States, as estimated in the balance of payments by US receipts for foreign use of IP, totalled $128.75 billion in 2019 (Bureau of Economic Analysis 2020b), or 0.6 percent of US GDP of $21.43 trillion (ibid., 2020a). Using the estimate of shrinkage in retail trade as a share of legal flows (1.62 percent) puts illegal disembodied technology flows out of the United States at about 0.01 percent of GDP, or around $2 billion per annum (see Table 1).

Considering actual damages awards that average about $100 million per year, this estimate would imply that substantially less than five percent of all cross-border trade secret theft is apprehended and restitution achieved through the courts. This is consistent with the general perception that what is caught is only the tip of the iceberg; however, the scale is now at least in a reasonable ballpark.

The suggested proxy approach results in a measure of illicit technology cross-border leakage that is substantially larger than what has been proven in the courts, which is consistent with the understanding that successful theft of trade secrets will not always be known to the victimized company and, even in cases where there is awareness, the case may not be pursued in the courts. At the same time, the suggested approach provides estimates that are plausible in light of what has actually been proven, in particular in light of the realistic expectation that the more valuable the trade secrets, the more stringent the measures that companies will take to protect them. This should ensure that most cases of trade secret leakage involve small values, which is consistent with the pattern of court awards. In the United States, courts make awards in about 50 percent of decided cases. With the number of cases filed running at about 1,400, and an annual

[4] An insightful story on this point concerns shoplifting of articles of minor value from high-end fashion stores. A store that put in place measures to prevent theft wound up catching clients who had bought large amounts of merchandise and felt “entitled” to walk away with a scarf or other object without paying. The embarrassment to their wealthy clients reduced sales, causing the store to remove the safeguards. The key point here is that profit-maximizing firms will tolerate a certain amount of shoplifting because it is, in fact, profit maximizing to do so. One result is that shoplifting remains not entirely negligible but a minor cost of doing business.

Table 1: Estimating International Leakage of Trade Secrets from the United States (2019)

	US$ in Millions or %	% of GDP
US receipts for use of IP (balance of payments)	$128,748	0.60%
Estimated shrinkage rate	1.62%	
Trade secret leakage	$2,086	0.0097%
Awards in trade secret litigation (total)	$105	
Restitution as % of leakage (maximum)	5.03%	
US GDP	$21,429,000	

Source: Bureau of Economic Analysis (2020a) for GDP and (2020b) for balance of payments data; Lex Machina (2020) for awards; and National Retail Federation (2020) for shrinkage rate.

Note: The maximum share of leakage that is recovered assumes all the awards were on cross-border trade secret theft; the actual share will have been lower.

average award total running at about $100 million, the mean award is in the order of $150,000.

The connection between trade secret theft and lost sales is far more tenuous. Generally speaking, technology does not flow easily across borders in disembodied form. For example, a vast amount of legally unencumbered technology in the form of expired patents is available to flow freely to less developed countries. However, this does not appear to happen. Casual empiricism informs us that most of the developing world is not operating at the technological level of the advanced societies at the turn of the millennium. The reason for this is that discrete elements of technology are not sufficient to launch a technologically sophisticated product that can compete with those produced in advanced countries. Typically, to acquire a new capability, a developing country would have to buy firms that possess the full package of necessary inputs, including patents, tacit knowledge and trade secrets (which may or may not be encoded and thus vulnerable to cyber theft), as well as skilled technical personnel. This is, after all, the way that firms in advanced countries acquire new capabilities: they seek out an active firm that has developed the desired product or capability and buy the firm (Ciuriak and Bienen 2014).

Discussion and Conclusion

The foregoing discussion has situated the rise in the significance of trade secrets in the technological context of the data-driven economy. Specific characteristics of IP in this economy — in particular the difficulty of using traditional IP measures to protect data and algorithms — make trade secrets regimes an increasingly important pillar of the IP protection framework. At the same time, the main source of leakage of trade secrets — intercorporate movement of key personnel — creates a conundrum for policy, given that the knowledge spillovers entailed in the movement of skilled personnel within an economy are critical to the dynamism of the economy. Since there is relatively little movement of skilled personnel internationally, this same consideration tempers concerns about international trade secrets leakage, notwithstanding the expansion in the ability to access trade secrets through breaches of digital security. Putting these considerations into a quantitative framework underscores that the potential leakage of value through trade secrets theft is orders of magnitude smaller than is presently asserted.

Several other considerations further temper concern over the trade secret theft across borders.

First, since most cases of theft are by former employees (Vasiu and Vasiu 2017), there is a reasonable question concerning the reality of allegations of theft, given the grey zone in which retained knowledge exists: what is normal tacit knowledge that is taken by an employee to a new job and what is truly a trade secret that is owed a fiduciary duty of protection? Further, given limited employee mobility across borders, this most frequent avenue for trade secret leakage is mostly domestic, in which case the damage to the national economy is limited (indeed, it tends to erode rents and intensify competition).

Second, advanced countries benefit from the brain drain out of developing countries. For example, foreign students with strong science, technology, engineering and math (STEM) skills contribute greatly to the development of technology in the United States that is branded as "American." China and India in particular play an important role in the global value chain of innovation through their legions of students with STEM skills overseas. It is quite likely — if not a near certainty — that the contribution these students (who often stay on as employees with technology companies in their host country) make to innovation in the advanced economies far exceeds any leakage of technology back to their home countries.

Third, any boost to technological advancement that developing countries receive from trade secret theft results in income gains that drive imports by these countries, including of technology. Notably, China, which stands accused of being responsible for most trade secret theft over the past few decades, was also the fastest-growing import market for goods ranging from Boeing jets to food products, but also for all manner of high-technology products, including computer chips. China also registered the steepest rise in payments for IP. To the extent that trade secret theft may help a company establish itself as a technology player, it quickly goes legal in order to play on the international stage where it must observe IP laws. Perhaps the biggest customer for legal computer technology in the world is Huawei, which spent $70 billion in 2018 buying components, including about $11 billion from US firms such as Qualcomm, Intel and Micron (see also Katz 2005, on the positive network effects of wide and expeditious dissemination of software, which may tip a market in favour of the supplier losing sales to piracy).

Fourth, and in a similar vein, the discussion of the impact of trade secret theft has implicitly been in a partial equilibrium setting (i.e., the costs of the theft to the owners). However, there are also likely general equilibrium effects at play. Put simply, if China were to successfully develop products based on technology stolen from the United States, it would probably be able to produce and sell the products more cheaply, which would increase competition and benefit not only consumers in China but also those in the United States. This same effect works, of course, at the national level, where domestic competition would be intensified to the benefit of consumers by the erosion of rents that trade secret leakage entails. Notably, unlike changes to legal regimes that affect incentives, there is no erosion of incentives to innovate from trade secret theft; rather, there is an incentive to strengthen a firm's safeguards.

Fifth, while trade secrets are becoming a more important part of firms' IP strategies in the data-driven economy, a major part of the growth in the value of IP assets protected by trade secrets law is in the form of proprietary data held by the world's most sophisticated firms, which are also best placed to protect their intangible assets. Indeed, strengthening trade secrets protection and enforcement may be counterproductive given the powerful tendency for market dominance in this modern economy.

To summarize, with the transition to a data-driven economy, trade secrets protection has become a much more important element in innovation policy. Trade secret theft is, in the first instance, a firm-specific shock; however, it also represents a knowledge spillover that has beneficial characteristics at the economy-wide level. When this knowledge spillover is across borders, trade secret theft becomes a source of international friction — and, indeed, allegations of frequent and systematic theft are central to the trade and technology war that is disrupting the global economy. At the same time, the analysis in this paper suggests that the widely cited estimates of trade secret theft of one–three percent of GDP are likely highly inflated, while a number of considerations mitigate the level of harm at the national level compared to the private harms experienced by firms whose trade secrets are stolen. Thus, while confirming the need to modernize the framework of IP protection to address the modern context for trade secret theft, the available evidence does not support a substantial expansion in the level of protection that legal frameworks currently provide; rather, it supports reform efforts to update and clarify the existing IP regime with a balanced perspective on protecting IP but also not undermining business dynamism and feeding unfounded international tensions.

Works Cited

Adler, Moshe. 2019. "Chinese Intellectual Property Theft: The Indictment of Huawei Is an Embarrassment." Counterpunch, May 31. www.counterpunch.org/2019/05/31/chinese-intellectual-property-theft-the-indictment-of-huawei-is-an-embarrassment/.

Almeling, David S. 2012. "Seven Reasons Why Trade Secrets Are Increasingly Important." *Berkeley Technology Law Journal* 27 (2) Fall: 1091–118.

Bagnall, James. 2011. "End of the line for Nortel." *Financial Post*, July 1. https://financialpost.com/technology/nortel-patents-sell-for-staggering-4-5-billion.

Barboza, David. 2011. "Motorola Solutions and Huawei Settle Claims Over Intellectual Property." *The New York Times*, April 13. www.nytimes.com/2011/04/14/technology/14huawei.html.

Black, Conrad. 2019. "Conrad Black: Trump is right to take on China, but Canada shouldn't extradite Meng." *National Post*, September 13. https://nationalpost.com/opinion/conrad-black-trump-is-right-to-take-on-china-but-canada-shouldnt-extradite-meng.

Blackwell, Tom. 2020. "Exclusive: Did Huawei bring down Nortel? Corporate espionage, theft, and the parallel rise and fall of two telecom giants." *National Post*, February 20. https://nationalpost.com/news/exclusive-did-huawei-bring-down-nortel-corporate-espionage-theft-and-the-parallel-rise-and-fall-of-two-telecom-giants.

Blair, Dennis C. and Jon M. Huntsman, Jr. 2017. *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*. Washington, DC: The National Bureau of Asian Research.

Bruns, Brittany S. 2017. "Criticism of the Defend Trade Secrets Act of 2016: Failure to Preempt." *Berkeley Technology Law Journal* 32: 469–501.

Bureau of Economic Analysis. 2020a. "Gross Domestic Product, Fourth Quarter and Year 2019 (Advance Estimate)." News release, January 30.

———. 2020b. "U.S. International Transactions, Fourth Quarter and Year 2019." News release, March 19.

CBC News. 1999. "Nortel in court over alleged 'brain drain' and lost trade secrets." CBC News, October 29. www.cbc.ca/news/business/nortel-in-court-over-alleged-brain-drain-and-lost-trade-secrets-1.183664.

CIPO. 2021. "What is a trade secret?" www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr03987.html.

Ciuriak, Dan and Derk Bienen. 2014. "Transplanting Economic Development: Don't Pick Winners, Buy Losers!" Discussion Paper. September 24. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2500419.

Columbus, Louis. 2019. "The Most Innovative Tech Companies Based On Patent Analytics." *Forbes*, December 15. www.forbes.com/sites/louiscolumbus/2019/12/15/the-most-innovative-tech-companies-based-on-patent-analytics/?sh=78369acb62ce.

Cooper, Sam. 2020. "Inside the Chinese military attack on Nortel." Global News, August 25. https://globalnews.ca/news/7275588/inside-the-chinese-military-attack-on-nortel/.

Courage, Noel and Janice Calzavara. 2015. "Protecting Trade Secrets in Canada." *Cold Spring Harbor Perspectives in Medicine* 5 (9): a024489.

D'Annunzio, P. J. 2020. "COVID-19 Bail Revoked in Case Over $550M Trade Secrets Theft From GlaxoSmithKline." *The Legal Intelligencer*, May 11. www.law.com/thelegalintelligencer/2020/05/11/covid-19-bail-revoked-in-case-over-550m-trade-secrets-theft-from-glaxosmithkline.

Desai, Shreya. 2018. "SHHH! It's a Secret: A Comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive." *Georgia Journal of International and Comparative Law* 46 (2): 481–513.

EUIPO. 2018. *The Baseline of Trade Secrets Litigation in the EU Member States*. Alicante, Spain: EUIPO.

Fischer, Eric A. 2005. *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. Congressional Research Service Report for Congress RL32777.

Freifeld, Karen. 2019. "U.S. charges Chinese professor in latest shot at Huawei." Reuters, September 9. www.reuters.com/article/us-huawei-tech-usa/u-s-charges-chinese-professor-in-latest-shot-at-huawei-idUSKCN1VU0J5.

Friedman, David D., William M. Landes and Richard A. Posner. 1991. "Some Economics of Trade Secret Law." *The Journal of Economic Perspectives* 5 (1) Winter: 61–7.

Glitz, Albrecht and Erik Meyersson. 2017. "Industrial Espionage and Productivity." IZA Discussion Paper No. 10816. Bonn, Germany: Institute of Labor Economics, June.

Griliches, Zvi. 1984. "Market Value, R&D, and Patents." In *R&D, Patents, and Productivity*, edited by Zvi Griliches, 249–52. Chicago, IL: University of Chicago Press.

Grimes, Steven and Shannon T. Murphy. 2018. “Summary Judgment Upheld in Favor of Competitor-Defendant Because Plaintiff Failed to Sufficiently Protect its Alleged Trade Secrets.” *Privacy & Data Security Law Blog* (blog), October 15. www.winston.com/en/privacy-law-corner/summary-judgment-upheld-in-favor-of-competitor-defendant-because-plaintiff-failed-to-sufficiently-protect-its-alleged-trade-secrets.html.

International Monetary Fund. 2019. “World Economic Outlook Database.” October. www.imf.org/en/Publications/WEO/weo-database/2019/October.

Johnson, Keith and Elias Groll. 2019. “The Improbable Rise of Huawei.” *Foreign Policy*, April 3. https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.

Katz, Ariel. 2005. “A Network Effects Perspective on Software Piracy.” *University of Toronto Law Journal* 55: 155–216.

Kemp, Richard. 2020. “Algo IP: Intellectual Property in AI Datasets, Insights and Outputs — the Growing Importance of Trade Secrets.” Lexology, June 16. www.lexology.com/library/detail.aspx?g=a6f36e7c-5908-4076-adf3-dfecb0c1d24d.

Leagle. 2018. “Quintel Technology, Ltd. v. Huawei Technologies USA, Inc.” www.leagle.com/decision/infdco20180118c29.

Lee-Makiyama, Hosuk. 2018. “Stealing thunder: Cloud, IoT and 5G will change the strategic paradigm for protecting European commercial interests. Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?” European Centre for International Political Economy Occasional Paper No. 2/18.

Lerman, Rachel. 2017. “Jury awards T-Mobile $4.8M in trade-secrets case against Huawei.” *Seattle Times*, May 18. www.seattletimes.com/business/technology/july-awards-t-mobile-48m-in-trade-secrets-case-against-huawei/.

Lester, Simon and Huan Zhu. 2020. “What Will the US-China Deal Accomplish on Tech Transfer, IP Protection and Innovation?” *Cato At Liberty* (blog), February 14. www.cato.org/blog/what-will-us-china-deal-accomplish-tech-transfer-ip-protection-innovation.

Levandoski, Stephen D. 2018. “To Seize the Initiative: Assessing Constitutional Due Process Challenges to the Defend Trade Secrets Act’s Ex Parte Seizure Provision.” *New York University Law Review* 93 (4) October: 864–902.

Lex Machina. 2018. *Trade Secret Litigation Report 2018*. Menlo Park, CA: Lex Machina. www.gordonrees.com/Templates/media/files/pdf/Trade_Secret_Litigation_Report_2018.pdf.

Leyden, John. 2004. “Cisco drops Huawei lawsuit: Legal attack called off.” The Register, July 29. www.theregister.com/2004/07/29/cisco_huawei_case_ends/.

Liebesman, Yvette Joy. 2017. “Ex Parte Seizures Under the DTSA and the Shift of IP Rights Enforcement.” *Business, Entrepreneurship & Tax Law Review* 1 (2) Fall: 390–412.

Linton, Katherine. 2016. “The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research.” *Journal of International Commerce and Economics* (September): 1–17.

McAfee and Center for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara, CA: Intel Security.

McWilliams, Gary. 2019. “Huawei Technologies loses trade secrets case against U.S. chip designer.” Reuters, June 26. www.reuters.com/article/us-huawei-tech-usa-verdict-idUSKCN1TR2YH.

Michel, Marissa, Craig Stronberg and Peter Geday. 2014. *Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats*. Center for Responsible Enterprise And Trade and PricewaterhouseCoopers. www.innovation-asset.com/hubfs/blog-files/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.

Mordaunt, Jeffrey, Neil Eisgruber and Joshua Swedlow. 2020. *Trends in Trade Secret Litigation Report 2020*. Chicago, IL: Stout.

National Retail Federation. 2020. *National Retail Security Survey 2020*. Washington, DC: National Retail Federation.

O’Connell, Donal. 2019. “The Increasing Importance of Trade Secrets and Trade Secret Asset Management Explained.” *Trading Secrets: A Law Blog on Trade Secrets, Non-Competes, and Computer Fraud* (blog), July 20. www.tradesecretslaw.com/2019/07/articles/trade-secrets/the-increasing-importance-of-trade-secrets-and-trade-secret-asset-management-explained/.

O’Keeffe, Kate and Aruna Viswanatha. 2020. “U.S. Drops Case Against Chinese Scientist at UVA.” *The Wall Street Journal*, September 23. www.wsj.com/articles/u-s-drops-case-against-chinese-scientist-at-uva-11600866354.

Png, I. P. L. 2017. “Law and Innovation: Evidence from State Trade Secrets Laws.” *Review of Economics and Statistics* 99 (1): 167–79.

Pooley, James. 2013. “Trade Secrets: the other IP right.” *WIPO Magazine*, June. www.wipo.int/wipo_magazine/en/2013/03/article_0001.html.

———. 2016. "The Myth of the Trade Secret Troll: Why the Defend Trade Secrets Act Improves the Protection of Commercial Information." *George Mason Law Review* 23 (4): 1045–78.

PricewaterhouseCoopers. 2018. "The scale and impact of industrial espionage and theft of trade secrets through cyber: Executive summary." Luxembourg: Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/b3b5fcfb-4541-11e9-a8ed-01aa75ed71a1/language-en/format-PDF/source-90181868.

Reisinger, Sue. 2020. "New Trade Secret Litigation Report Shows Cases Down But Damages Up in 2019." Law.com, April 21. www.law.com/corpcounsel/2020/04/21/new-trade-secret-litigation-report-shows-cases-down-but-damages-up-in-2019/?slreturn=20200824172154.

Richards, Gregory, Laurent Mirabeau, Jonathan Calof and Muriel Mignerat. 2014. "A Process View of Organizational Failure: The Case of Nortel." *Academy of Management Annual Meeting Proceedings* (1): 17411–411.

Roach, Stephen. 2019. "Is China Really Cheating?" BNN Bloomberg, January 15. www.bnnbloomberg.ca/is-china-really-cheating-1.1198892.

Sagara, Yuriko. 2019. "Big Data Protection under Unfair Competition Prevention Act has just started in Japan." Nakamura & Partners, Legal Updates, July 8. www.nakapat.gr.jp/en/legal_updates_eng/big-data-protection-under-unfair-competition-prevention-act-has-just-started-in-japan/.

Sandeen, Sharon and Christopher B. Seaman. 2017. "Toward a Federal Jurisprudence of Trade Secret Law." *Berkeley Technology Law Journal* 32: 829–913. https://open.mitchellhamline.edu/facsch/428.

Saunders, Kurt M. and Nina Golden. 2018. "Skill or Secret? — The Line Between Trade Secrets and Employee General Skills and Knowledge." *New York University Journal of Law and Business* 15 (1): 61–99.

Silverman, Ed. 2014. "Wire Fraud Charges Against Former Lilly Scientists are Dismissed." *The Wall Street Journal*, December 8. www.wsj.com/articles/BL-270B-1145.

Statt, Nick. 2020. "Self-driving car engineer Anthony Levandowski pleads guilty to stealing Google trade secrets." The Verge, March 19. www.theverge.com/2020/3/19/21187651/anthony-levandowski-pleads-guilty-google-waymo-uber-trade-secret-theft-lawsuit.

Thomas, Katie. 2016. "5 Accused of Stealing Drug Secrets From GlaxoSmithKline." *The New York Times*, January 20. www.nytimes.com/2016/01/21/business/5-accused-of-stealing-drug-secrets-from-glaxosmithkline.html.

United States Department of Justice. 2015. "Kolon Industries Inc. Pleads Guilty for Conspiring to Steal DuPont Trade Secrets Involving Kevlar Technology." Press release, April 30.

———. 2019. "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice." Press release, January 28.

United States Patent and Trademark Office. 2020. "Trade secret policy." www.uspto.gov/ip-policy/trade-secret-policy.

Vasiu, Ioana and Lucian Vasiu. 2017. "Backdoor Man: A Radiograph of Computer Source Code Theft Cases." *Journal of High Technology Law* XVIII (1): 1–37.

von Kalinowski, Julian O. 1961. "Key Employees and Trade Secrets." *Virginia Law Review* 47 (4) May: 583–99.

Wajsman, Nathan and Francisco García-Valero. 2017. *Protecting Innovation through Trade Secrets and Patents: Determinants for European Union Firms*. Alicante, Spain: EUIPO. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf.

WIPO. 2019. *World Intellectual Property Indicators 2019*. Geneva, Switzerland: WIPO. www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2019.pdf.

———. 2020. "Frequently Asked Questions: Trade Secrets." www.wipo.int/tradesecrets/en/tradesecrets_faqs.html.

WTO. 2020. *United States — Tariff Measures on Certain Goods from China*. WT/DS543/R. September 15.

Yap, Chuin-Wei, Dan Strumpf, Dustin Volz, Kate O'Keeffe and Aruna Viswanatha. 2019. "Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics." *The Wall Street Journal*, May 25. www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.

Zhang, Laney. 2019. "China: Trade Secret Provisions Under Anti-unfair Competition Law Revised." Global Legal Monitor, June 6. www.loc.gov/law/foreign-news/article/china-trade-secret-provisions-under-anti-unfair-competition-law-revised/.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline