Guardians of Intellectual Property in the 21st Century: The Global Supply Chain Industry

Steven Carnovale
Rochester Institute of Technology

Jessica Carnovale
Rochester Institute of Technology

Doug Strub
The National Bureau of Asian Research

Alison Szalwinski
The National Bureau of Asian Research

Jonathon Marek
The National Bureau of Asian Research

Abstract

The length and complexity, the number of geographically distributed firms, as well as the number of products that modern supply chains are tasked with delivering to consumers have grown exponentially over the past several decades. Regional supply chains have transformed into global ones with intellectual property and related proprietary information being dispersed across firms' extended enterprises. Couple these trends with the increase in digitization and the larger presence of internet-enabled technologies, and the number of attack vectors for malevolent actors has outpaced potential protections and safeguards. Succinctly stated, supply chains are vulnerable to intellectual property theft. But questions remain, such as which parts of supply chains are the most vulnerable? What technologies exist to help protect intellectual property? What is missing, and what can be done? Hence the purpose of this paper. Upon investigation, our team has found: (1) The implementation of training for supply chain personnel to the scale and scope of the increasingly pervasive vulnerabilities of IP in supply chains; (2) The

implementation of protocols for traceability and tracking of raw materials at the beginning of the supply chain, and across entities of the supply chain, ideally through an established set of standards for IP protections in the onboarding process; and (3) establishing a 'detection/mitigation/recovery' risk management footing such that firms have a balanced approach to handling IP theft.

Introduction

Supply chains are the primary value-creating engines of the modern economy, working in the background to provide the world with the goods it needs to survive. Generally speaking, supply chains handle the identification and acquisition of raw materials and services; the production, manufacturing, and distribution of finished and work-in-process goods and services to manufacturing locations; and the movement and storage of finished products from the source of production to the end consumer.

In the early years after the industrial revolution, supply chains were, at most, national, though predominantly subnational. Over the past few decades, however, they have grown considerably longer, more complex, and much more global in nature. No longer are firms constrained by geography when they look to source a part or service. Now, advances in telecommunications and freight technologies have opened up access to every corner of the world. Couple this access with increased levels of regional economic integration through reductions in trade barriers, including through preferential trade agreements, and companies can now access markets that previously would have been impossible. For both consumers and manufacturers alike, this is a boon. Consumers gain access to a more diverse set of goods at a lower price, and manufacturers can take advantage of the lower cost of labor and greater access to raw materials.

Despite these major economic benefits, the globalization of supply chains has also introduced new risks. Among the myriad vulnerabilities that such technological shifts engender, one lurking threat stands out: the real, and growing, risk of IP theft. IP is defined by the World Intellectual Property Organization as creations, both tangible and intangible, resulting from human intellect.[1] Such creations are generally protected by patents, copyrights, trademarks, and other legal protections to safeguard against infringement on the inappropriate use or the exploitation of someone else's property. As supply chains have lengthened and become more global, firms' IP has been exposed to threats unimaginable several years prior. For example, a report from the Commission on the Theft of American Intellectual Property

at the National Bureau of Asian Research (NBR) echoed this point regarding lengthening supply chains:

> [S]tolen IP represents a subsidy to foreign suppliers that do not have to bear the costs of developing or licensing it. In China, where many overseas supply chains extend, even ethical multinational companies frequently procure counterfeit items or items whose manufacture benefits from stolen IP, including proprietary business processes, counterfeited machine tools, pirated software, etc.[2]

The risk that firms operating in or along global supply chains face with respect to IP is extremely pervasive. In a survey by the American Chamber of Commerce in Shanghai, 54% of companies (all of which are foreign companies operating in China) believed that "lack of IP protection and enforcement" is a hindrance to their business.[3] This belief was most common in the pharmaceutical, medical devices, and life sciences industry, at 71.4%, followed closely by industrial manufacturing, at 68.4%. Indeed, this threat is not imaginary. The Commission on the Theft of American Intellectual Property calculated that "the annual losses are likely to be comparable to the current annual level of U.S. exports to Asia—over $300 billion."[4] The problem is so vast that public-private partnerships have cropped up to protect the most vulnerable industries (i.e., those connected to the defense industrial base or critical technologies). One recent example features the intelligence community and the U.S. Defense Advanced Research Projects Agency partnering to create systems to protect IP along the semiconductor supply chain.[5] However, this risk is not limited solely to the most cutting-edge industries, such as semiconductors. An automotive supplier, for example, working with a major original equipment manufacturer that may digitally receive highly confidential schematics for a new part it is manufacturing introduces cybertheft risks to the IP. Another significant risk is the degree to which the Internet of Things (IoT) connects devices via cloud computing but also exposes serious security threats and vulnerabilities. This is not anecdotal. A recent Deloitte report finds that cybertheft and related incidents are vastly up, particularly during the Covid-19 pandemic.[6]

Furthermore, all functions across the supply chain are vulnerable to IP infringement. Manufacturing, either internally or through contracted third parties, often involves unique and proprietary production processes, rich with IP all too vulnerable to theft via corporate espionage. Firms have established manufacturing joint ventures in various parts of the world where leakage of IP renders them vulnerable to exploitation and extremely expensive remediations (i.e., ransomware). The 2018 Section 301 report

estimates that from China alone, "theft of American IP currently costs between $225 billion and $600 billion annually"—a figure that aligns with the findings of NBR's Commission on the Theft of American Intellectual Property.[7,8]

Cumulatively, both anecdotal reports as well as empirical findings continue to point to the supply chain as a unique vulnerability in the war against IP infringement. In order to provide clarity on this issue, we address the following questions:

1. Which parts of the supply chain (i.e., sourcing, manufacturing, and outbound logistics) are the most vulnerable, and what can be done to secure them?
2. What is the current state of the technological arsenal to fight IP theft, and are there gaps?
3. What best practices can companies leverage to mitigate IP risks?

Where Are the Largest Vulnerabilities?

In February 2021, President Joe Biden signed Executive Order 14017, which seeks to strengthen U.S. supply chains through a comprehensive review of their vulnerabilities. The executive order directs agency heads to focus on "the defense, intelligence, cyber, homeland security…or other contingencies that may disrupt, strain, compromise, or eliminate the supply chain—including *risks posed by supply chains' reliance on digital products that may be vulnerable to failures or exploitation*" (emphasis added).[9] Given the increasing utilization of technology in modern supply chains, cybersecurity threats continue to mount, and the consequences of a breach are massive. In 2020 the average cost of a data breach was $3.86 million, with the average resolution time 280 days, and with healthcare facing the highest average cost.[10] This is a serious issue when considering the degree to which healthcare relies on IP (e.g., drug formulations, vaccine development, and various other R&D initiatives). In fact, the FBI has recently partnered with the National Intellectual Property Rights Coordination Center on several initiatives, one of which explicitly focuses on the inclusion of counterfeit goods into the Department of Defense (and other federal) supply chains.[11] Clearly, the threat that modern supply chains face is gaining greater attention among policymakers.

A Cross-Functional Supply Chain IP Issue

It does not matter which component or function of the supply chain is being examined, there is one constant: people are ultimately responsible for planning, execution, and safeguarding of supply chain assets and, consequently, IP. In all of the interviews with experts from the field

conducted for this report, in one way or another regardless of experience working in supply chain management, one critical vulnerability kept arising: the human factor.

Trade secrets are not always kept in a folder marked "TOP SECRET" in an executive's office. Rather, these secrets—proprietary knowledge or information, often related to the processes of design and production inherent to supply chains—often reside in the skill and talent of the personnel employed at the company. This expertise is multifaceted: (1) the skill/talent for which the employee was hired, (2) the decision-making fiat that the employee has, and (3) the skill and talent accumulated on the job. Bad actors often seek to extract and exploit proprietary information existing in the form of employees' knowledge and skills. At the same time, vulnerabilities arise out of to whom, and how much, decision-making authority is delegated to employees, who might then make choices that expose IP and other digital assets to the risk of theft. There are two overarching vulnerabilities in this space: the human factor and subversion of process-based controls.

The human factor. The double-edged sword of talented employees is that they are hard to acquire, and when acquired, they are hard to keep. With respect to IP, the difficulty is related to what occurs when employees depart the firm that owns the IP, or has used or otherwise been exposed to IP as part of the supply chain. This poses risks associated with employees taking proprietary processes and ideas with them, or being vulnerable to other malevolent actions from outside entities. A typical strategy is to employ legalese and build noncompete, nondisclosure, or other contractual measures to hedge against such breaches. But these measures do not always work.

Subversion of process-based controls. Conventional strategy to protect IP generally deals with protecting patents, copyright protections, and trade secrets. In the United States, such protections are enumerated in the Constitution. Article I, Section 8, provides Congress the power "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[12] In fact, the first U.S. patent was issued in 1790. While the application and vetting processes have changed, the legal structure of ownership rights have not.

Copyright protections are generally related to creative pursuits (e.g., art and multimedia), whereas patent protections relate to the invention and novelty of an industrial product.[13] Trade secrets are a form of IP that is commercially valuable and contains confidential information on a product or process (e.g., the recipe for a food product).[14] In the case of a patent or a copyright, each mechanism's purpose is to act as a process-based control to

protect the owner of the intellectual property, whereas a trade secret represents an internal protection of sorts. Yet, the mere application for a patent, for example, could signal to a malevolent actor that the submitting firm has something worth stealing, thereby exposing the firm to vulnerability. Some experts even suggest not filing a patent at all![15] Further, consider where and how management stores proprietary information. Take, for example, information that explicitly details how a new manufacturing process will be executed, or an R&D document detailing the features of a company's new smartphone. Is the information stored on hard disks internally, or on cloud servers externally? Who has access? What about the transition from one cloud storage provider to another? What if a schematic for a patent submission has been sent to a printer that has random access memory, thereby opening up an access point for a hacker to siphon off IP? In each of these instances, for a supply chain to effectively produce products and maintain its competitiveness, all IP along the supply chain needs to be secured and protected. Unfortunately, the expansiveness of modern supply chains makes this a challenging proposition. A recent Deloitte report sums up the problem rather succinctly: "Advancements in technology, increased mobility, rapid globalization, and the anonymous nature of the Internet create growing challenges in protecting trade secrets."[16]

IP Issues in Sourcing

Sourcing refers to managing the external resources of a firm. This includes the identification and acquisition of raw materials, work-in-process inventory, maintenance/repair/operating inventory, internet services, and logistics services, among other resources. In most cases, the sourcing function is the "start" of the supply chain; it is also where the risks to IP begin. In interviews conducted for this report, a few relevant themes for IP and sourcing kept arising. Broadly speaking, these issues are related to traceability and counterfeit goods. An important point to note is that these concepts are two sides of the same coin, but manifest at different times in the sourcing process. Generally speaking, a lack of traceability with respect to raw materials or other work-in-process inventory causes (or at least facilitates) the inclusion of counterfeit goods into the supply chain. A somewhat recent and rather notable example of the balance between traceability and counterfeiting is the "horsemeat scandal" at various supermarkets in Ireland and the United Kingdom. After the Food Safety Authority of Ireland began inspecting the DNA of various frozen meat products amid suspicion of deceptive practices, it was revealed that over one-third of the "beef" samples contained horsemeat and nearly 85% contained pig DNA.[17] The supermarket Tesco chain later came under scrutiny when one

of the ready-made meal products (spaghetti with "beef" Bolognese) was found to contain 60% horsemeat.[18] The meal was sourced from a French factory, whose suppliers were spread out across Europe, extending the geographic and administrative length of the supply chain to a point where fraud and deception become veritably impossible to root out. Thus, the challenge of traceability makes the issues related to the human factor noted above even more pronounced, as IP in the supply chain requires trust between partners, even when there are contractual considerations involved. This issue is only amplified by the complexity associated with protecting trade secrets, industrial design, or other more technologically dependent IP.

Traceability. The challenge of ensuring transparency in the supply chain, particularly as it relates to the inbound source of raw materials, presents issues of quality control. For manufacturers that rely primarily on trust in their suppliers not to incorporate fraudulent products, the inclusion of substandard materials can easily become a problem. As supply chains continue to expand their supply bases globally, this risk only increases. The consequences for quality, resulting from a lack of transparency, can be grave.

The pharmaceutical industry provides a rich context to examine the importance of this issue. Various products rely on temperature-controlled delivery and storage, in addition to strict quality standards throughout the supply chain. In addition, this industry is also subject to the lengthening and globalization of supply chains as "roughly 80% of active pharmaceutical ingredients and 40% of finished drug product are imported into the U.S. from overseas."[19] In order to enhance traceability and strengthen protections, President Barack Obama in 2013 signed into law the Drug Supply Chain Security Act, which "outlines steps to build an electronic, interoperable system to identify and trace certain prescription drugs as they are distributed in the United States. This law enhances the ability of the Food and Drug Administration (FDA) to protect consumers "from exposure to drugs that may be counterfeit, stolen, contaminated, or otherwise harmful." It also improves "detection and removal of potentially dangerous drugs from the drug supply chain to protect U.S. consumers." Additionally, the law directs the FDA to establish "national licensure standards for wholesale distributors and third-party logistics providers, and requires these entities report licensure and other information to FDA annually."[20] Effectively, the legislation "require[s] drug supply chain stakeholders to trace prescription drugs, in a secure manner, from the manufacturer down to the dispenser of the drug" in order to improve overall traceability and ensure the integrity of the pharmaceutical industry.[21] While the Drug Supply Chain Security Act is quite helpful, it only covers one sector. This law can, however, present a

framework for an industry-wide standard (which will be discussed further in subsequent sections).

Counterfeited goods. With respect to inbound materials, there is no coherent standard to verify the authenticity of a raw material (e.g. traceability), and as a result, potentially also the product itself. This gives rise to significant opportunities for infringement of a product's IP. One assessment by the FBI suggests that "counterfeit goods cost the U.S. economy an estimated $600 billion a year, or 3% of the U.S. gross domestic product."[22] The counterfeit issue arises as a result of a lack of transparency and the opacity of information being shared across supply chain entities and manifests in increased warranty, liability, and service costs to manufacturers.

IP Issues in Manufacturing

The manufacturing portion of supply chains is chiefly tasked with transforming raw materials and work-in-process inventories into finished goods for ultimate distribution to consumers. In the sequencing of a supply chain, this part of the process would be subsequent to the sourcing function, and as a result what happens in the manufacturing processes of firms is largely dependent on what is being acquired externally. Therefore, the issues raised above in the sourcing process implicitly affect the manufacturing process. But there are additional considerations—specifically, issues related to product quality, brand image, and data security.

Product quality. As manufacturing continues to globalize, and as firms engage contract manufacturers more and more frequently, they can leave themselves vulnerable to theft of IP on the process side. There are also risks to theft of IP on the product itself, particularly related to reverse-engineering. The consequences of fraudulent or subpar quality inputs into the production process can have serious consequences to the original equipment manufacturer, often arising out of warranty expenses and other related quality failures. If the parts entering into the final product are of poor quality, this could compromise the end product, resulting in serious financial and reputational loss. Consider the potential liability and reputational risk that firms can face if an input to a product is fraudulent.

The Takata airbag recall is an excellent example of this. In the early 1990s, Takata, a major airbag supplier to several automakers, switched the chemical composition of the component required to create the deployment of its airbags. This new chemical composition, when exposed to prolonged heat and humidity, can deteriorate and cause the airbag to deploy too soon, or not at all, leading to serious injury or death. In the mid-2000s an internal report indicated that Takata knew that this could and likely would happen, but the company covered up the finding and continued to supply numerous

automakers with fraudulent and inferior products. After multiple deaths and injuries and several million recalled airbags, Takata pled guilty to criminal charges. The economic cost to resolve the issue was approximately $24 billion, which was four times greater than Takata's revenue forecasts.[23] This was not just an issue for Takata, as the company's poor-quality products resulted in Toyota, Mazda, Subaru, and BMW also entering into agreements totaling over $550 million for the losses encountered by their customers.[24]

Brand image. The negative impact on brand image that arises from IP infringement and related maladies also can be dire for firms. The rise in platforms such as Amazon, Alibaba, and related online marketplaces have simultaneously increased access to markets and consumers and opened up new pathways for malevolent actors to sell counterfeit goods fraudulently listed as genuine. Increased levels of drop-shipping (a customer fulfillment approach where products go directly from the manufacturer/distributor and bypass a retail or other intermediary with the goal of decreasing lead times to the customer) have obfuscated the clarity of ownership and enabled "passing of the buck" with regard to who is legally at fault.

Take, for example, a fraudulent product sold to an unknowing consumer via Amazon through a third-party reseller. The reseller never physically owns or holds the good but merely processes the order and then facilitates shipping to the end consumer. Is the platform responsible for verifying the authenticity of the product? Is the reseller? Is the shipping company? Is the brand? Ultimately, regardless of who is responsible, the brand image can be jeopardized. This cuts both ways: on the product side and on the platform side. From an IP standpoint, a firm has a vested interest in protecting its brand via the channels through which its products get distributed. On the other hand, unless there is traceability and strict governance between manufacturer and retailer, once the ownership of the product has transferred this issue becomes challenging to police. Consumers also "punish" the platform that sold the product, and this may well be justified if the platform knowingly allowed counterfeit goods to enter its distribution channels. Yet, the issue becomes even murkier if it was the brand that allowed a counterfeit product into circulation in the first place.

Data security. A final issue that arises in the context of IP infringement and manufacturing is data security. This issue largely arises in collaborative manufacturing environments where joint engineering teams work together on a schematic/computer-aided design or other digital medium through which the product is developed. It is conceivable that product design and engineering teams from all corners of the world simultaneously tap into a common server that is hosted in the cloud, which is allegedly secure. On the one hand, it is a marvel of modern technology to be able to co-develop a

product leveraging talent across the world. On the other hand, the IP housed on these servers is an increasing cybersecurity vulnerability, the costs of which are enormous and increasing. Malevolent actors seek to gather software code, patented trade secrets, or other potentially valuable information that they can exploit for their gain.

There are effectively two key points of concern about data security with respect to IP. First, as global supply chains continue to lengthen geographically, and the number of agents to whom a firm grants access continues to grow, more and more confidential and proprietary data must enter a cloud-based environment to allow collaboration between entities. Second, there is seldom appropriate onboarding to govern the handling of proprietary data, as well as other data security concerns, thus exposing firms to a major IP vulnerability. These issues are unrelenting and will likely grow exponentially over the coming decades.

IP Issues in Outbound Logistics and Delivery

The outbound logistics function of the supply chain is responsible for the movement of goods, either from the raw material source to the manufacturing facility or from the manufacturing facility to its next destination (i.e., distribution center, retail establishment, or final consumer), and storage in between. Here, international borders are crossed, government agencies are interacted with, and intermediary connections are made. The storage element occurs in between each phase of the movement, where warehouses act as repositories for products yet to be sold, or yet to be transformed into a finished good. As supply chains have lengthened and globalized, few areas of the supply chain have been stretched and tested as much as the logistics space. As a result, these processes are uniquely vulnerable to malevolent actors. Issues of title, ownership, liability, and information security pervade this space. Third-party logistics providers act as guardians of information but are susceptible to hacking and can be complicit in the inadvertent facilitation of theft and leakage of IP. In the logistics space, two prominent threats arise: data security and product guardianship.

Data security. While data security in the above section referred to specific IP associated with the product itself, here it refers to IP around process and delivery. IP around delivery deals with strategy: design and deployment of logistics networks, and the processes associated with how a product will arrive at the consumer. Strategy includes plans for developing a new distribution center, any trade secrets associated with product allocations to a free-trade zone, or even the rebalancing of work-in-process inventory to a new intermediary location.

Take, for example, recent innovations around UPS's drone delivery where there is IP for the technology to optimize scheduling and the design of the drone itself. The issue of safeguarding data and ensuring its security is an immense challenge for logistics professionals, particularly because of the volume and variety of products being moved. The adoption of IoT technology to increase connectivity and access to information via microchip and internet-enabled devices has led to severe new vulnerabilities for IP theft. Necessarily, IoT increases the connection points and thus the exposure to theft. This increased exposure creates complexity, which tends to be a significant driver of fraudulent activity and can lead to vulnerabilities such as spoofed data about product shipments, sensors on transportation that are hacked, and shipments that are hijacked, facilitating theft of products and their resultant IP (through reverse-engineering).

Product guardianship. In the ever-expanding space of logistics and freight, ownership terms and liability can get messy. While shipment terms (i.e., free on board—when ownership and assumption of risk are transferred when the product is placed onboard the vessel of the buyer's choice; or free alongside—where the assumption of risk is transferred when the product is placed adjacent to the vessel of the buyer's choice, usually at the port of departure) are pre-negotiated, and International Commercial Terms can help facilitate the transaction, the guardianship of the product is significantly more opaque.

Recall the issue with fraudulent or subpar quality products entering the production process. When products sit in warehouses, if left unmonitored, they are vulnerable to shrinkage. This shrinkage can lead to malevolent actors either reverse-engineering products and flooding the market with discounted, poor-quality products or replacing original products with lower-quality alternatives. If the product being reverse-engineered is a finished good, there are issues associated with brand image, quality, and warranty concerns, as noted above. The essential issue is that there is often ambiguity associated with who will interact with the products, thus exposing firms to IP-related vulnerabilities, despite any contractual governance (or perhaps lack thereof) that may be in place. All told, logistics as a function is highly vulnerable to IP theft.

State of Technology for Supply Chain IP Protections

Today, most IP resides in a digital medium (i.e., servers and onsite computers). As such, a breach of a firm's IP often implies that there has been a breach of a firm's cyber defenses and security practices. Coupled with the increased complexity of supply chains and IP residing in distributed systems across multiple firms, this is a recipe for theft and malevolence. What options currently exist to deal with IP theft from a technology perspective? Broadly

speaking, the existing technology seeks to protect a firm's security footing in order to mitigate potential malevolent actors from cybertheft (e.g., ransomware attacks and IP theft), technology that safeguards proprietary information, and finally technology to identify when a breach has occurred. These three areas are discussed in this section.

Cybersecurity Protections

According to a report from Deloitte, "compared with more familiar cybercrimes such as the theft of credit card, consumer health, and other personally identifiable information…IP cyber theft has largely remained in the shadows."[25] A concerning thought, but a practical reality, is that IP is the largest asset for most companies, and it may be the most vulnerable. The distributed nature of work and recent trends in the work-from-home landscape have exacerbated the challenges associated with cybertheft of IP. Thus, in order for any digital asset to be secured across a firm's extended enterprise (including its IP), a comprehensive cybersecurity protocol must be implemented. Currently, the following is recommended:

- ✓ Enable encryption, where possible, such that in the event of a cyberattack the IP is harder to access.
- ✓ Perform stress tests and employee training around cybersecurity defense. As the human factor was seen as one of the most critical vulnerabilities in IP, such investments in training should help to mitigate IP theft.
- ✓ Assess the scope and location of all IP throughout the extended enterprise, and develop a counterintelligence footing, anticipating the threat and preparing the response.[26]
- ✓ Practice cyber hygiene by applying the National Institute of Standards and Technology framework to identify vulnerable digital assets; protect, where possible, against vulnerabilities; and detect and respond to incidents quickly and comprehensively.[27]

Blockchain Technology

As of late, supply chains and blockchain have made quite the alliance, with recent reports predicting the "post-COVID-19 blockchain supply chain market to grow from USD 253 million in 2020 to USD 3,272 million by 2026, at a Compound Annual Growth Rate (CAGR) of 53.2% during 2020–2026."[28] While not specific to IP per se, blockchain technology can be useful to IP in many ways. Effectively, the value of blockchain technology is by its design: it is a distributed ledger that records entries and transactions in such a way that they are resistant to fraud, as the preceding transactions are immutable, and all subsequent transactions are recorded in the ledger.[29] This technology

allows for a certain degree of anonymity through the use of hashing and cryptography so as to anonymize the entry, theoretically facilitating a heightened degree of information sharing by hiding identifying information. Blockchain technology also allows for the use of so-called smart contracts, which are self-governing, and recording contracts that record all relevant legal information in an immutable way.

Of course, the popular press is replete with examples of blockchain technology being applied to cryptocurrencies and in other related contexts, but the real potential is in its traceability. Consider an example of verifying the authenticity of a copyrighted or patented product whose IP is vital to its owner. Let's assume that the product is sold on a popular platform where third parties can join and sell products. Blockchain technology can be used as a mechanism where the owner logs the ownership and relevant details of the product on the blockchain, then the platform (or consumer) can subsequently check the current product against the information on the blockchain so as to verify its authenticity. In this scenario, the blockchain serves as a potential tool to authenticate the product and theoretically protect the IP of the owner. Recent patents have been issued, in fact, that allow for name authentication and legal responsibility mechanisms through blockchain.[30] But not all jurisdictions allow blockchain as proof of ownership.

Artificial Intelligence

Artificial intelligence (AI) refers to computerized attempts to model, emulate, and perform human (or biological) intelligence. The World Intellectual Property Organization defines AI as "a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention."[31] Applications are vast. AI has been used to detect illicit behavior ranging from fraudulent purchases to national security threats, as well as for facial recognition and even in logistics to monitor and track delivery driver behavior.

In the context of IP, significant attention has been paid to AI recently. Legal questions over ownership of AI-generated inventions, the way in which AI should be protected, and so on have stimulated a passionate and ongoing debate. The core of the arguments rest on the antecedent of the "creation," given that the AI that is driving the innovation is being programmed by humans. As a tool for IP protection, however, AI can be useful. Recently, it has been utilized in compliance management, providing more accurate real-time information so that decision-makers are operating more efficiently. AI has also been used to provide proof of origin, product tracking, and authentication by augmenting the hashing and cryptography algorithms so

that they can be applied more broadly to other IP such as video, images, and audio. Generally speaking, leveraging the power of modern computing to automate compliance tasks can significantly increase throughput and improve overall fraud detection. This, coupled with the power and traceability of blockchain is likely to be a game changer with respect to IP protections.

From Current State to Future State

What Are the Current Gaps, and What Should Be Done?

Recent data from the Organisation for Economic Co-operation and Development (OECD) suggests that trade in counterfeit goods represents approximately 3.3% of world trade, with the United States being the country most affected.32 This is a particularly concerning issue amid the escalating frequency and cost of cyber breaches targeting firms' IP. The current state is precarious.

The questions of where the gaps are and what should be done can be answered in one word: cohesion. There are piecemeal solutions to every problem addressed in this report. For example, consider the traceability problem with raw materials in the sourcing of coffee beans. Blockchain is a possible solution to ensure traceability of the coffee bean from farm to cup, and everywhere in between. Yet, who will bear the cost? The family farmer located in a developing country? The logistics firm tasked with moving the raw coffee beans from farm to market? The brand that ultimately will sell the roasted, ground, or brewed coffee beans? What about the question of responsibility for counterfeit goods being sold on an ecommerce platform? Of course, if resources were not an issue the platform could deploy AI-driven technology to weed out such products before they are sold, ban the seller from the platform, and remediate the concerns of the consumer. Clearly, this is not the case.

The anecdotal examples above illustrate the reason that cohesion—the development of a cohesive strategy for tackling IP theft—is such a challenge. It is not that there is a lack of possible protections. The real challenge is how to tie them together, when to use which approach, and who will bear the cost. Our experts identified this problem of agency as well. Their recommendations are distilled in the following subsection.

Key Recommendations for How to Protect IP in Supply Chains

The findings of the report and the interviews with industry experts provided for a broad swath of recommendations across all areas of the supply chain, from sourcing to outbound logistics. The common theme that was mentioned, regardless of a person's location or position in the supply chain,

was the critical role that the human factor plays in IP infringement in supply chains. This led to one overarching and critical recommendation:

Training. One of the experts with whom we spoke said it best: "Training personnel for what to look out for in the supply chain is essential. The soft skills become critical." Increased interconnectedness and dependence between firms upstream and downstream in the supply chain means that vulnerabilities around IP leakages are increasingly heightened. Thus, training employees to correctly handle and protect IP is no longer optional; it is necessary. Supply chain personnel need to understand what IP is, where the vulnerabilities are, where IP resides, how to protect it, and what the cost of a breach is. Currently, supply chain personnel are largely unaware stakeholders in the governance of IP protections. This passive inattention to IP likely arises from the fact that its protection is normally entrusted to a legal department. Yet, as has been outlined in this report, multiple parties (many of whom function squarely within traditional supply chain domains) should have responsibility over its protection. This needs to change to a more proactive, awareness-focused approach. In the technologically focused world in which supply chains are entrenched, malevolent actors have more touch points, more unique attack vectors, and more opportunity than ever before. The entities operating in the supply chain are the first lines of defense for securing the intellectual capital and property of organizations.

A "detection, mitigation, and recovery" approach. In all cases and functions of the supply chain, protecting IP in supply chains boils down to risk management. One of the experts who provided feedback responded that "IP compliance is risk mitigation, and this is a necessary component," while another suggested that "there needs to be proper risk management and risk assessment that is focused on IP protection." Generally speaking, there are three categories into which such strategy falls: (1) detection, (2) mitigation, and (3) recovery.[33] Across all functions of the supply chain, the following recommendations are advanced.

Detection. Detection starts at the source, and as such the sourcing function acts as the gatekeeper for preventing fraudulent/subpar products from entering the production process. The following measures are needed to strengthen detection:

- ✓ *Make IP a priority during the supplier selection process by including key metrics and stage gates around potential traceability protocols, fraud detection, or other IP protections in the selection of suppliers*.
- ✓ *Implement supplier scorecards that include a measure of "IP defense" to secure IP in future transactions*.
- ✓ *Leverage and implement AI and other computerized technology to detect fraudulent products and materials where possible*.

- ✓ *Increase information sharing as a formal requirement of partnering with a firm.*
- ✓ *Integrate systems to help improve information sharing. The current patchwork of systems, technologies, and processes that are operating disparately renders supply chains vulnerable to IP infringement and theft.*

Mitigation. Mitigation activities assume (rightfully so) that IP infringement will likely occur and plan for the best ways to manage the fallout. First, enhanced enterprise-wide data security is critical for reducing IP leakage. This was a common and strongly held view in all the interviews conducted with experts, and several problems were identified. Schematics on the production and sourcing side are vulnerable. Product routing and shipping details are accessible via IoT devices in freight, and therefore susceptible to outside attacks. Employees' email accounts, for example, that are accessible via their phones or tablets open up entirely new attack vectors. This is not anecdotal, as recent reports indicate that over 50% of IP breaches are achieved through email.[34] Thus, recommendations for achieving data security are (fortunately) largely congruent with several known cybersecurity recommendations:

- ✓ *Catalog what data is being stored and who has access to it and establish a mechanism for tracking when such data has been accessed.*
- ✓ *Maintain a register for data. While it might seem obvious, this is a crucial first step in protecting data.*
- ✓ *Maintain redundant cloud and physical backups of key data.*
- ✓ *Leverage encryption wherever possible.*

Another important set of recommendations focus on augmenting the supplier onboarding process to include specific cybersecurity requirements to safeguard data and other proprietary information. This will hedge against (though of course not eliminate) malevolent actors being able to easily acquire IP via a firm's supply base. Specifically, firms should implement the following measures:

- ✓ *Take the internal data security recommendations noted above and evaluate the degree to which suppliers are adhering to them, or the degree to which they maintain their own standards that are congruent with your internal data security standards.*
- ✓ *Include specific IP considerations, such as IP information governance policies (i.e., data security), access and use policies (particularly when IP is not being accessed at the focal firm's facilities but rather at an*

offsite location), security protocols around background checks to gain access to IP, and storage.

- ✓ *Evaluate and enumerate the potential damages of IP theft, both financially and reputationally, and prepare a disaster response plan on how to approach it.*
- ✓ *Establish a coherent legal strategy for remediation that includes a cross-functional team.*

Recovery. The goal of a recovery plan is to return to a pre-disruption state. As such, recovery strategies are needed to chart a path forward after attack. The following measures would help facilitate recovery:

- ✓ *Use redundant suppliers and diverse sourcing strategies.*
- ✓ *Establish backup systems and other contingency plans to move forward.*
- ✓ *Execute the legal strategy outlined above and develop plans to communicate with the affected parties (e.g., suppliers and customers).*

Conclusion

As this report has shown, supply chains are highly vulnerable to IP theft. The length and complexity, the number of firms, the number of countries, and the number of products that modern supply chains are tasked with sourcing, manufacturing, and ultimately delivering to consumers have grown exponentially over the past several decades. Regional supply chains have transformed into global ones with IP and related proprietary information being dispersed across firms' extended enterprises. Couple this with the increase in digitization and the greater presence of internet-enabled technologies, the number of attack vectors for malevolent actors has outpaced potential protections and safeguards.

Unfortunately, there is no part of the supply chain that is unaffected by these threats. Sourcing must focus on quality by training personnel on what to look for and how important traceability is to ensure compliance with quality standards and authenticity. Manufacturing must act as a backstop on sourcing to ensure that subpar quality or inauthentic materials do not enter into the production process, potentially causing quality failures at later stages of the supply chain. Outbound logistics should buttress data security in a meaningful way to protect against external interference into the IP contained in shipments. In sum, a cohesive, coordinated approach is essential to ensure that IP is protected to the highest degree possible.

Authors

Steven Carnovale, Ph.D. is a Professor of Supply Chain Management at the Saunders College of Business at the Rochester Institute of Technology (RIT). Prior

to joining RIT, Dr. Carnovale was Nike Professor of Supply Chain Management at Portland State University. Dr. Carnovale is a supply chain strategist and econometrician specializing in supply chain analytics, risk management, and global sourcing/production networks with a specific focus on network optimization. He currently serves as Editor-in-Chief of the Journal of Purchasing and Supply Management, an Associate Editor at the Journal of Supply Chain Management, and Rutgers Business Review. He has published in the Journal of Supply Chain Management, the Journal of Business Logistics, the Journal of Purchasing and Supply Management, International Journal of Production Economics, Journal of International Business Studies, the European Journal of Operational Research and Annals of Operations Research among others. Dr. Carnovale earned his B.S. and PhD degrees at Rutgers University, specializing in Supply Chain Management and Marketing Sciences. Dr. Carnovale is a frequent speaker at academic and professional supply chain meetings on topics related to supply networks & analytics, with a specific focus on how firms can use these concepts to generate enhanced visibility and performance within their extended enterprises.
email: scarnovale@saunders.rit.edu

Jessica Carnovale is a Visiting Lecturer of Supply Chain Management at the Rochester Institute of Technology, Saunders College of Business. She has a BA in Business Management from William Paterson University and a Masters of Legal Studies with a concentration in Global Trade Law & Compliance from the Rogers College of Law, at the University of Arizona. Jessica spent 11 years in retail banking and compliance before transitioning to global trade/logistics as a customs broker. Jessica has also served on the board of directors for the Rochester, NY Institute of Supply Management (ISM) chapter, serves as Faculty Advisor to the APICS@RIT student group, and has recently authored an appendix to a National Bureau of Asian Research (NBR) study focusing on global trade policy and intellectual property in supply chain management.
email: jcarnovale@saunders.rit.edu

Doug Strub is Assistant Director with the Center for Innovation, Trade, and Strategy at NBR. Mr. Strub manages and supports research for Trade Center projects focusing on Asian economic, trade, innovation, and intellectual property policy issues. He served as co-editor of the NBR Special Report "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order," and authored the introduction to the "Navigating China's Growing Digital Influence" roundtable in Asia Policy (vol. 16, no.2). Prior to joining NBR, Mr. Strub spent five years in China working for the American Chamber of Commerce in Shanghai, writing reports for the World Bank in Beijing, and studying Mandarin in Guilin and Wuhan. He received his MA in International Affairs from the George Washington University's Elliott School of International Affairs.
email: dstrub@nbr.org

Alison Szalwinski is Vice President of Research at NBR. Ms. Szalwinski provides executive leadership to NBR's policy research agenda and oversees research teams in Seattle and Washington, D.C. She is the author of numerous articles and reports and co-editor of the Strategic Asia series along with Ashley J. Tellis and Michael Wills, including the most recent volumes, Strategic Asia 2020: U.S.-China Competition for Global Influence (2020), Strategic Asia 2019: China's Expanding Strategic Ambitions (2019), and Strategic Asia 2017–18: Power, Ideas, and Military Strategy in the Asia-Pacific (2017). Prior to joining NBR, Szalwinski spent time at the U.S. Department of State and the Center for Strategic and International Studies. Her research interests include U.S. alliance relationships, U.S.-China relations, and the implications of great-power competition for U.S. alliances in the region. She holds a BA in Foreign Affairs and History from the University of Virginia and an MA in Asian Studies from Georgetown University's Edmund A. Walsh School of Foreign Service.
email: aszalwinski@nbr.org

Jonathon Marek is a Project Associate with NBR's Center for Innovation, Trade, and Strategy. In this role, he supports the Center's work on digital trade governance, intellectual property, 5G, supply chains, and other trade and economic strategy topics in Asia. He served as co-editor of the NBR Special Report "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order" and co-author of the NBR Backgrounder "A Concise Guide to Huawei's Cybersecurity Risks and the Global Responses." Jonathon is a graduate of Georgetown University's Walsh School of Foreign Service, where he majored in international political economy with a Chinese minor and Asian studies certificate. His academic interests include the role of economic statecraft in grand strategy; the intersection of technology, trade, and national security; and the political economy of trade policy.
email: jmarek@nbr.org

***Acknowledgement**: This article is the product of a report commissioned by the National Bureau of Asian Research's Center for Innovation, Trade, and Strategy to study the risks to intellectual property (IP) in modern supply chains, and to understand what can be done to protect them. All of the following is directly from the original report and all requisite permissions have been granted to the authors for its reprinting in its current form. The primary research methodology was modeled after a semi-structured interview approach, such that issues could emerge naturally. Thereafter, the findings were synthesized into a series of concrete insights and recommendations. Nine experts participated in three roundtable interview sessions between October 2020 and January 2021 in order to solicit expertise and insight. In each case, all interviews were held virtually. The interview protocol was set ahead of time, and was standardized to match and align with the stated project objective and outcomes. Each session was recorded with the participants' permission, and ahead of time the participants were made aware that the meeting was being governed by Chatham House Rule. All quotes enumerated in the report below are presented anonymously and have been edited for clarity and*

for concision of message. In all cases, the interviews lasted approximately 90 minutes. Any questions regarding copyright of this report should be addressed to dstrub@nbr.org.

Endnotes

1. World Intellectual Property Organization. (2016). *Understanding Intellectual Property* (2nd ed.). Geneva, Switzerland: WIPO.
2. Commission on the Theft of American Intellectual Property. (2013). *The IP Commission Report*. Seattle, WA: National Bureau of Asian Research.
3. AmCham Shanghai. (2020). *2020 China Business Report*. Shanghai, China.
4. Commission on the Theft of American Intellectual Property. (2013). *The IP Commission Report*. Seattle, WA: National Bureau of Asian Research.
5. Mendoza, N. F. (2021, March 21). Intel and DARPA partner to advance U.S. semiconductor supply chain security, domestic manufacturing. *Tech Republic*.
6. Nabe, C. (n.d.). Impact of COVID-19 on cybersecurity. *Deloitte*.
7. Office of the U.S. Trade Representative. (2018, March 22). Findings of the investigation into China's Acts, Policies and Practices related to Technology Transfer, Intellectual Property, and innovation under section 301 of the Trade Act of 1974. Washington, DC: Office of the U.S. Trade Representative.
8. Commission on the Theft of American Intellectual Property. (2013). *The IP Commission Report*. Seattle, WA: National Bureau of Asian Research.
9. White House Briefing Room. (2021, February 24). *Executive Order on America's Supply Chains by Joseph R. Biden Jr., 2/24/2021* [Transcript].
10. Zorabedian, J. (2020, July 28). What's new in the 2020 cost of a data breach report. *Security Intelligence*.
11. White-collar crime: Intellectual property theft/piracy [Organization website]. (n.d.). *Federal Bureau of Investigation.*
12. *The Constitution of the United States: A transcription - Article. I. Section. 8*. (n.d.). The U.S. National Archives and Records Administration.
13. World Intellectual Property Organization. (2016). *Understanding Intellectual Property* (2nd ed.). Geneva, Switzerland: WIPO.
14. About IP: Trade secrets [Organization website]. (n.d.). *World Intellectual Property Organization.*
15. Forbes Technology Council. (2018, July 23). 10 Effective ways to protect your intellectual property. *Forbes*.
16. Gelinne, J. P., Fancher, D., & Mossburg, E. (2018, July 23).The hidden costs of an IP breach: Cyber theft and the loss of intellectual property. *Deloitte.*
17. Lawrence, F. (2013, February 15). Horsemeat scandal: The essential guide. *The Guardian*.
18. Horsemeat scandal: Tesco reveals 60% content in dish. (2013, February 11). *BBC*.
19. Pagliarulo, N., & Lopez, E. (2018, April 23). Top challenges facing drug supply chains. *BioPharma Dive*.
20. Drugs: Drug Supply Chain Security Act (DSCSA) [Organization website]. (2022, March 9). *U.S. Food and Drug Administration.*
21. Smith, C. (2019, April 2). INSIGHT: The Drug Supply Chain Security Act and preemption of state laws. *Bloomberg Law.*
22. Schlessinger, J., & Day, A. (2019, March 13). Here's how the trade war could lead to a boom in counterfeit goods. *CNBC*.
23. Takata puts worst-case recall costs at $24 billion. (2016, March 29). *Bloomberg.*

24. Jones, C., & Bomey, N. (2017, June 25). Timeline: How Takata's air-bag scandal erupted. *USA Today*.
25. Gelinne, J. P., Fancher, D., & Mossburg, E. (2018, July 23).The hidden costs of an IP breach: Cyber theft and the loss of intellectual property. *Deloitte*.
26. Behr, A., & Slater, D. (2021, August 24). Intellectual property protection: 10 Tips to keep IP safe. *CSO from IDG Communications*.
27. Cybersecurity Framework [Organization website]. (n.d.). National Institute of Standards and Technology.
28. Research and Market. (2021, March). *Global Blockchain Supply Chain Market by Offering (Platform, Services), Type (Public, Private, Hybrid & Consortium), Provider, Application (Asset Tracking, Smart Contracts), Enterprise Size, Vertical (FMGC, Healthcare), and Region—Forecast to 2026.* Dublin, Ireland: Research and Markets.
29. Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers and Industrial Engineering,* 154(6), 107130.
30. Future FinTech Group Inc. (2021, March 4). Future FinTech granted blockchain technology-related software copyrights from the China National Copyright Administration. *Cision PR Newswire*.
31. WIPO Secretariat. (2020, May 21). *WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI): Second Session*. World Intellectual Property Organization.
32. Trade in fake goods is now 3.3% of world trade and rising. (2019, March 18). *OECD*.
33. DuHadway, S., Carnovale, S., & Hazen, B. T. (2019). Understanding risk management for intentional supply chain disruptions: Risk detection, risk mitigation, and risk recovery. *Annals of Operations Research, 283*(1), 179–98.
34. Egress. (2019). *Data Privacy in 2019 Research Report*. London, U.K.: Egress.