LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 1 | Issue 2

2023

INTELLECTUAL PROPERTY THEFT- A NATIONAL SECURITY ISSUE

Panya Sethi[1]

I. ABSTRACT

Theft of intellectual property refers to the unlawful taking of any creative work, concept, trade secret, or sensitive information that is protected by intellectual property laws. Theft of intellectual property (IP) covers a broad spectrum of wrongdoing, from trademark and copyright violations to patent infringement.[2] Intellectual property theft may be devastating to individuals, companies, and governments that have spent years perfecting their work. Theft of intellectual property severely slows economic growth and innovation. The rapid expansion of digital infrastructure and resources has, unfortunately, made it simpler for cybercriminals to steal, copy, and distribute valuable intellectual property. The stakes are higher, and the demand for strict protection and enforcement of intellectual property is expanding as a result. Because the rightful owner of an IPR is able to prevent others from making use of the protected material, such rights are often referred to as "negative rights." When a party other than the IPR owner or a person authorized by the IPR owner to use the right (a licensee) acts in a way that is inconsistent with the IPR, this is known as an infringement. Intellectual property infringement comes in many forms, and it's important for lawyers, company owners, and shareholders to understand each one and how they may be prevented. Having a patent on an invention gives the creator the right to prevent others from profiting from their creation without permission. Copyright laws and trademark laws both aim to safeguard creative works against imitation. Protected works can always sue to prohibit others from copying or adapting them without permission. By definition, the holder of an IPR can

[1] Student, Symbiosis Law School, Noida

[2] What Is Intellectual Property Theft?, PROOFPOINT, https://www.proofpoint.com/us/threat-reference/intellectual-property-theft#:~:text=Intellectual%20property%20(IP)%20theft%20is,protected%20under%20intellectual%20property%20laws. (Accessed Nov 10, 2022).

forbid anybody else from profiting from the protected work without first obtaining the IPR holder's consent.

II. KEY WORDS:

Infringement, intellectual property, unauthorized use.

III. WHAT IS IP THEFT?

If you take or use someone else's ideas without their permission, you are committing intellectual theft.

Any original work of authorship, any novel technique of production with measurable economic worth, and any commercially useful unique mark, such as a name, symbol, or logo, are all examples of intellectual property. Ideas and assets protected by copyrights, trademarks, patents, or trade secret laws are examples of intellectual property. The term "intellectual property" can refer to a wide variety of things, including client lists, mechanical innovations, poetry, logos, and more. Copyrights on artistic endeavors like music, photos, and poetry, as well as patents for innovations and trademarks for commercial markings or branded items, all fall under the umbrella of intellectual property. The laws of each individual state and the United States as a whole provide protection for intellectual property.

The United States Trade Representative (USTR) conducted an investigation of Chinese IP laws and practices under the Trump administration, finding that some of them violated Section 301 of the Trade Act of 1974. The United States responded with a World Trade Organization lawsuit and tariffs on Chinese products worth billions of dollars. China responded with its own tariffs on US imports and a challenge to the US's tariffs at the World Trade Organization. In January of 2020, the United States and China finalized their "Phase One Agreement.", which addressed some of the parties' trade and intellectual property disputes. The Phase One Agreement, however, did not address fundamental issues, such as coercive technology transfer. The emergence of the Coronavirus Disease 2019 (COVID-19) pandemic has heightened tensions between states and slowed progress

toward a Phase Two Agreement, despite the parties' expectations for additional discussions.

IV. TYPES OF IP THEFT

- **Patent infringement**: Patents issued by organizations like the USPTO or EPO may be incorporated into a product or used in its production, in commercial contexts. without the permission of the patent owner, this is considered patent infringement. A famous case law under this is **Pfizer vs Teva Pharmaceuticals (TEVA) & Sun Pharma (2013).** Another fascinating case was Pfizer vs. Teva, in which generic medication companies paid damages for the first time after selling a generic version of a drug for which the patent had not yet expired. This is what people mean when they talk about a "at-risk launch." Generic versions of Pfizer's best-selling acid reflux drug Protonix were introduced by Teva and Sun Pharma in 2007 and 2008, respectively. In 2011, the drug's patent was slated to expire. Of the total $2.15 billion granted by Pfizer, the companies have reached settlements with Teva and Sun Pharma for $1.6 billion and $550 million. Since Takeda's Nycomed licensed the patent to Pfizer's Wyeth, the two companies are related, Takeda received 36% of the settlement.[3]
- **Trademark infringement**: When a third party uses a mark that is identical to a registered trademark without permission to do so in commerce (often in connection with comparable or rival goods), trademark infringement occurs when a mark is used that is confusingly similar to a registered mark, leading consumers to believe the products are produced by or sold by the trademark holder. For decades, two significant institutions have fought over the trademark "apple" in the case of **Apple Corps v. Apple Inc**.[4] Eight years before Steve Jobs started Apple Inc., the Beatles had their own record label called

[3] Singh, Vipin. "10 Largest Initial Patent Infringement Awards in the US." *GreyB*, 7 March 2021, https://www.greyb.com/blog/largest-patent-infringement-awards/ . (Accessed 22 November 2022)
[4] "Examples of Trademark Infringement Cases." *UpCounsel*, https://www.upcounsel.com/examples-of-trademark-infringement-cases . (Accessed 22 November 2022).

Apple Corps. Following a lawsuit filed by the Fab Four, Jobs settled out of court by agreeing not to work in the music industry. Nonetheless, Apple Inc. was once again sued after the introduction of iTunes. Jobs ultimately purchased Apple Corps' trademark rights and leased them back to the firm in order to resolve the issue.

- **Copyright infringement:** For the most part, when a literary, cinematic, or musical work (and sometimes a technical manual) is reproduced (in whole or in part) in connection to the original work, or when a derivative work comprises, numerous significant sections derived from the original work, this constitutes an infringement of copyright. Over the last several years, federal penalties for copyright infringement have increased in severity. Anyone found guilty of copyright infringement faces a maximum sentence of three years in jail and a fine of $250,000. The sentence increases to 10 years in jail if it can be shown that the infraction resulted in private financial benefit or commercial advantage. Infringing on someone's copyright includes actions like downloading music without permission, posting someone else's work online without permission, using pirated software, and plagiarizing someone else's work without making substantial changes.[5]
- **Trade secret violation:** Although trade secrets are rarely explicitly protected by law, when they are shared between businesses, it is common practice for both to sign NDAs to protect the information. A party in violation of an NDA is one that acquires confidential information belonging to another and then makes that information public or utilizes it for commercial purposes without the owner's permission. Definitions of what constitutes "confidential information" are fundamental to any NDA. Intentionally disclosing a company's trade secrets is a crime. It is unlawful to acquire a trade secret by

[5] Rittenberg, Julia, and Adam Ramirez. "What is Copyright? Everything You Need to Know." *Forbes*, 22 June 2023, https://www.forbes.com/advisor/business/what-is-copyright/ . (Accessed 22 November 2022).

means such as breaking a non-disclosure agreement, engaging in industrial espionage, stealing, fraud, or bribery. Misappropriation occurs, for instance, when an outsider gains unauthorized access to a company's computer system and steals its trade secrets. You may be guilty of misappropriation if, after signing an NDA, you are restricted to using company computers while handling sensitive information, you used your own laptop in a public area one weekend to do some work.

- **Counterfeit:** In certain places, such as the European Union (EU), there is no clear legal distinction between infringement of products and counterfeit goods, whereas in others, this distinction is clear. In cases where there is a discrepancy, counterfeit products must breach an intellectual property right and also be colorable imitations of the genuine goods, making the definition narrower than that for trademark infringement. What this means is that the counterfeit item itself must seem like a fake to the average buyer. Criminal penalties for trademark infringement may include up to ten years in prison and a fine of up to two million dollars. If a trademark is utilized on counterfeit goods or services, monetary penalties may be levied. Together, INTERPOL and Europol made the largest-ever seizure of counterfeit food components last year. Dangerous quantities of counterfeit goods were confiscated, including "nearly nine tons of fake sugar contaminated with fertilizer" and "eighty-five tons of olives 'painted' with copper sulphate solutions to enhance color." Many counterfeiters were apprehended around the world, since the web of participants stretched across several countries.[6]

V. EXAMPLES OF IP THEFT

- **Electric vehicle manufacturers dispute over stolen trade secrets.**

[6] "5 Examples of Dangerous Counterfeit Products." *Scout CMS*, 24 January 2017, https://www.scoutcms.com/news-and-views/5-examples-of-dangerous-counterfeit-products . (Accessed 22 November 2022)

Two electric car manufacturers are at odds over alleged IP theft. To protect its proprietary information, Tesla filed a lawsuit against an electric SUV maker. According to Tesla, 70 staff defected to Rivian Automotive and took proprietary information with them.[7]

- **Biotech company employee steals data on the third attempt**

The security system of a corporation should do more than only prevent intellectual property theft; it should also sound an alarm if an employee tries to steal confidential information. During his career, Rongzan Ho worked with AbbVie. He took confidential information about the production of medicine with him when he quit and went to work for a rival business, Alvotech. Ho made two attempts while working at AbbVie to send himself emails containing confidential corporate information, but both times were unsuccessful due to AbbVie's security measures. On his third try, he supposedly succeeded, and he took that knowledge to Alvotech.

- **Company IP stolen by its inventor.**

While it is possible to restrict an employee's access to the company's resources, doing the same for the creator of the company's intellectual property may be more difficult. Corrosion Prevention Technologies sued the firms it said had stolen trade secrets by developing competing versions of its CorrX product. It's unclear how the former employees stole the company's data, but it appears that a confidentiality agreement was the only safeguard in place.

VI. WHAT ARE THE LEGAL CONSEQUENCES OF 'IP THEFT'?

When determining monetary penalties (and an award for damages) for civil IP rights violations, local laws are considered. Generally speaking, punitive damages are rarely given in many common law jurisdictions or the European Union (EU), with a few

[7] Groot JD and Brook C, "IP Theft: Definition and Examples" (*Digital Guardian* December 16, 2021) <https://digitalguardian.com/blog/ip-theft-definition-and-examples > (Accessed 22 November 2022)

significant exceptions. In order to be awarded punitive or exemplary damages, a plaintiff must often show that they suffered real or anticipated financial loss as a result of the infringement. Since proving a significant financial loss can be difficult, courts in many countries can sometimes award a fair royalty (that would have been payable by a hypothetical licensee) instead of damages. According to Chinese intellectual property law, defendants can be punished with monetary fines in the form of statutory judgments. Relevant elements in determining the amount and kind of damages may include, but are not limited to, those set out by the applicable jurisdiction:

- A deliberate choice on the part of the violator;
- The sum of money they made off of the infraction;
- The total amount of license payments that the rightful owner might have earned but did not because of the infringement, or
- Whether or not there is available competition for goods that do not infringe.

In many cases, the priority of IP owners is to put an end to infringement rather than seek monetary compensation. Consequently, when trying to stop an illegal infringement, it is usual practice to file an injunction first and then pursue a claim for damages.

A. DEFENSES FOR IP THEFT IN US

- **Lack of intent:** If the accused did not set out to steal the IP or use it for their own benefit, then they cannot be found guilty of IP theft under the statutory definition of the crime.
- **Lack of ownership rights:** It is impossible to file a claim for infringement if the person accusing the defendant of IP theft does not have ownership rights to the IP

in question. If intellectual property laws were unable to protect the content, the same logic would apply.[8]

- **"Unclean hands":** A person who does this is doing improperly and should be held accountable for their actions. It would be considered "unclean hands" if the person waited a long time after learning of the intellectual property infringement before filing a lawsuit."
- **Fair use:** The accused infringer of intellectual property may assert fair use as a defense in such a situation. The intellectual property can be used for teaching purposes without violating the fair use clause. It's recommended that you consult with an intellectual property attorney when attempting a fair use defense, as the process can be intricate.

VII. HOW DOES IP THEFT HAPPEN?

Internal actors pose the greatest risk to a company's IP. While accidental IP theft by employees is always a possibility, most insider attacks are carried out on purpose.

Such insiders may include:

- To put it bluntly, disgruntled workers who utilize their position of power to try to bring down the company they will soon be leaving.
- When workers leave one firm for another, they often seek for perks that will help them land a better position at their new organization.
- Individuals recruited to act as employees of one organization in order to steal proprietary information and leak it to another are known as "double agents."

[8]"Intellectual Theft: Everything You Need To Know" (*UpCounsel* October 27, 2020) <https://www.upcounsel.com/intellectual-theft > (Accessed November 10, 2022)

Contractors, vendors, or software used by an organization that has access to confidential information is also at risk of theft.[9]

VIII. MALICIOUS INSIDER THEFT EXAMPLES

- **Departing employees:** Virtually always pose a risk to the privacy of sensitive information due to the level of access they have to the data and the expertise they possess. Even after an employee has left an organization, they still pose a threat through insider assaults, whether through negligence or malice. Malicious insider threats might arise in the form of vengeful ex-employees who feel wronged by an involuntary employment leave.[10] With a heart full of resentment, they take advantage of their final hours of access to the system to destroy or corrupt vital information, destroying the company's operations. A medical device packaging firm in Atlanta encountered the former scenario.[11] the month of March 2020. In retaliation for his COVID-related termination, an ex-employee hacked his former company's database, I made unauthorized changes to approximately 115,000 computerized shipping records and deleted another 2,300. After making these changes, he removed the phony account, thereby blocking any chance of restoring the PPE supplies originally ordered.

- **Double agents:** The term "malicious insider threat" refers to an insider who poses as an employee at a corporation but is actually working for or on behalf of an outside entity to leak confidential information. The perpetrators of these crimes utilize the stolen information for personal gain, internal corporate sabotage, or fraudulent activity. As the October 2020 Amazon incident showed, not even the

[9] "What Is IP Theft and How to Prevent It from Happening" (*Spirion* July 21, 2022) <https://www.spirion.com/blog/what-is-ip-theft-and-how-to-prevent-it-from-happening/ > (Accessed November 10, 2022)
[10] "Understanding Malicious Insider Threat Examples to Avoid an Insider Attack" (*Spirion* November 15, 2021) <https://www.spirion.com/blog/malicious-insider-threat-examples /> (Accessed November 10, 2022)
[11] "Former Employee of Medical Packaging Company Charged with Sabotaging Electronic Shipping Records "(*The United States Department of Justice*April 16, 2020) <https://www.justice.gov/usao-ndga/pr/former-employee-medical-packaging-company-allegedly-sabotages-electronic-shipping >(Accessed November 10, 2022)

largest corporations with the largest information security resources are immune to the threat posed by malevolent insiders. While keeping mum on the attack itself, the company did notify affected customers that an employee had leaked their email addresses to a third party.

- **Third-party insider threats**: Anyone with authorized access to sensitive information can be a malevolent insider; they don't even have to be an employee of the firm being attacked.

IX. MITIGATING THE RISK OF A MALICIOUS INSIDER ATTACK

- The first step is sensitive data discovery, which locates and catalogs all the private information stored within an organization, including in networks, endpoint devices, the cloud, and individual inboxes. As such, you will have a good idea of what you need to keep an eye on for any signs of strange behavior that may indicate the presence of a malevolent insider. After an assault, discovery can help you determine with high certainty what was taken, changed, or destroyed so you can take appropriate action.
- After collecting all of your data, you may organize it in useful ways. Data classification is the process of organizing sensitive data into categories according to several factors, such as the degree to which the data is sensitive and the data privacy regulation(s) to which it must adhere. As a result, there will be less potential for information to be illegally accessed, altered, exposed, or damaged. Classification can aid in identifying the perpetrator of an attack if one occurs.

A **data remediation tool** is the missing piece of the puzzle, as it prevents sensitive data from being stolen during transport. If data has been maliciously altered, classification can determine what kind of fix should be made to it immediately, such as in the case of an insider attack.

X. HOW CAN AN IP OWNER PREVENT 'IP THEFT' ABROAD?

The greatest strategy to reduce the likelihood of IP infringement is to get protective designations for it in countries other than the owner's. In this sense, most nations have ratified several WIPO treaties, streamlining the process by which domestic IP rights can be extended to new jurisdictions. For instance, the Patent Cooperation Treaty streamlines the process by which a patent can be extended to other jurisdictions if certain conditions are satisfied. Extending the protection of a trademark through the Madrid System involves the same steps as those involved in the original registration.

The PCT's primary objectives are to aid applicants in securing worldwide patent protection for their inventions, to aid patent offices in awarding decisions, and to aid the public in gaining access to a wealth of technical information about these breakthroughs. PCT allows applicants to file a single patent application that will be considered for patent protection in a large number of countries. However, there are times when filing with a national or regional patent office, like the European Patent Office, is the best option for extending protections (EPO).[12]

XI. BEST PRACTICES COMPANY CAN ADOPT TO PREVENT IP THEFT

Security measures against intellectual property theft can be difficult to implement if they have unintended consequences, such as impeding on workers' ability to get legitimate work done. You may fulfill both requirements by keeping a sharp eye out for suspicious behavior and putting a stop to it before any damage is done.

Here are seven best practices a business can use to safeguard intellectual property and provide workers more leeway to maximize productivity.

- **Create Acceptable Use Policies**

[12] Zyl CV, "Luxembourg: What Is Intellectual Property 'Theft' And How To Avoid It?" (*Mondaq* October 1, 2020) <https://www.mondaq.com/trademark/990102/what-is-intellectual-property-39theft39-and-how-to-avoid-it > (Accessed November 10, 2022)

The first step toward curbing IP theft is establishing policies that spell out who within your organization is authorized to access company data and under what circumstances that data may be shared. After that, make the rules easily accessible to anybody who would need to see them (including workers, contractors, and other stakeholders) in order to ensure that they are followed.[13]

For example, electronic copies of the policies could be made available to stakeholders and made mandatory reading on the lock screen of company laptops.

- **Maintain Transparency with Employees and Contractors**

One way to stop intellectual property theft is to be open with workers and outside contractors about the data you have on them. It's also required by law in some places, such as New York and California, where businesses are required to be transparent about their surveillance practices.

For these two reasons, as well as the moral necessity of openness in business dealings, it is recommended that employers make it clear what data they collect on their employees, how they collect it, and whether or not the data is shared with outside parties. Furthermore, openness fosters a trustworthy environment. When security and workers regard one another as partners in safety, workers are more likely to report suspicious activity or admit when they themselves have made a mistake. Better security practices may be fostered across the board by reflecting on and learning from past blunders in this area.

- **Monitor all of your data and its movement.**

It is more practical and time-efficient to classify all data as prospective IP and track its journey without first determining which types of data qualify as IP. Considering that the

[13] "What Is Intellectual Property (IP) Theft?" (*Code42* November 9, 2022) <https://www.code42.com/blog/what-is-intellectual-property-theft/ > (Accessed November 10, 2022)

average user's data is exposed inadvertently 34 times per day, it is sensible to treat every data as intellectual property and safeguard it accordingly.

Make it clear to your staff that keeping tabs on how much sensitive information leaves the building and goes to places that can't be trusted isn't the same thing as spying on them When compared to monitoring activities, tracking keystrokes, collecting photographs of screens, studying performance, and other intrusive acts, Protecting the company's innovation and competitive edge via vigilance over the data it stores is in everyone's best interest. The monitoring of data also creates an audit trail that can be used to look into an IP incident. With this tool, you can establish a "baseline" of normal occurrences from which to identify suspicious changes that may indicate IP risk.

Last but not the least, monitoring data travel automatically is crucial, given the impossibility or high difficulty of manually labeling and implementing policies to restrict data transfer. Furthermore, your technologies should sound the alarm if data is moved in ways that might point to IP threats.

- **Flag your most at-risk IP**

Know what intellectual property is vulnerable to theft so you can take precautions against it. Find out where your company's trademarks, patents, trade secrets, and other sensitive data are stored and how vulnerable they are to theft. Implementing this procedure is critical as it allows for optimal allocation of theft prevention resources. Furthermore, The "noise" may be reduced with its aid.

Within data monitoring activities, by isolating high-risk information and ignoring less-critical warnings, but still potentially harmful, data. Manually identifying sensitive IP is, like data monitoring, not practical for most enterprises. In order to monitor the risk behavior associated with the information at risk in real time, you will need technologies that can automatically recognize where such information is located.

- **Stop breaches before they happen**

An ounce of protection against intellectual property theft is worth more than four and a half million dollars in remediation. Preventing infractions from occurring may save a firm a lot of money in the long run by reducing the likelihood of having to pay fines, repairing damaged brand reputation, and replacing lost competitive advantages. Maintaining security shouldn't impede the flow of information within your organization, or else sharing and collaborating will be a hassle. Instead, make it a priority to secure critical data and prevent breaches without interfering with day-to-day operations.

- **Situationally train and drive secure work habits**

A startling 96% of American security managers and experts agree that their organization has to do more to boost data security education and awareness. Rather than relying on long movies or training techniques that staff will ignore as an annual "checklist item," interactive programs will yield better results in education.

If you time your training sessions properly, you'll get far better results. By providing training at the precise moment an employee is about to perform anything that might compromise data, for instance. Patented data being uploaded to an unauthorized server? Limit the fallout and advise the worker to read up on what constitutes appropriate sharing. The security team may teach the staff themselves or physically distribute the movies, but they are constantly responding to urgent situations. Employees should be trained proactively and reactively, ideally using an automated system that can be tweaked to match specific needs and organizational structures.

- **Use the right tools**

The proper tools must be deployed in order to detect vulnerable IP and track potentially harmful data transfers. In addition, If you want to stop potential breaches from happening, you need software that notifies you immediately of any detected risks. Automated tools are necessary for protecting IP assets at scale in organizations where employees work in a mobile, flexible, fast, and dynamic environment.

XII. CONCLUSION

 (ISSN: 2583-7753)

IP theft can have long-term negative consequences for a corporation. Companies lose a lot of money due to intellectual property theft, and they often have to spend much more money on their own to fix the damage and prevent it from happening again due to costly lawsuits and other legal actions, and reputational damage for companies. Preventing intellectual property theft and mitigating damages, such as developing policies in the company for people responsible for accessing data, maintaining transparency with employees and contractors, identifying the most vulnerable intellectual property, and preventing breaches from occurring, would help protect the company's reputation and save them money.

XIII. REFERENCES

- What Is Intellectual Property Theft?, PROOFPOINT, https://www.proofpoint.com/us/threat-reference/intellectual-property-theft#:~:text=Intellectual%20property%20(IP)%20theft%20is,protected%20under%20intellectual%20property%20laws. (Accessed Nov 10, 2022).
- Kevin J. Hickey et al., INTELLECTUAL PROPERTY VIOLATIONS AND CHINA: LEGAL REMEDIES FEDERATION OF AMERICAN SCIENTISTS (September 17, 2020), https://sgp.fas.org/crs/row/R46532.pdf (Accessed Nov 22, 2022).
- Singh, Vipin. "10 Largest Initial Patent Infringement Awards in the US." *GreyB*, 7 March 2021, https://www.greyb.com/blog/largest-patent-infringement-awards/ . (Accessed 22 November 2022)
- "Examples of Trademark Infringement Cases." *UpCounsel*, https://www.upcounsel.com/examples-of-trademark-infringement-cases .(Accessed 22 November 2022).
- Rittenberg, Julia, and Adam Ramirez. "What is Copyright? Everything You Need to Know." *Forbes*, 22 June 2023, https://www.forbes.com/advisor/business/what-is-copyright/ . (Accessed 22 November 2022).

- "Trade Secret Infringement & Potential Legal Defenses | Intellectual Property Law Center." *Justia*, 15 October 2022, https://www.justia.com/intellectual-property/trade-secrets/infringement/ . (Accessed 22 November 2022).
- "5 Examples of Dangerous Counterfeit Products." *Scout CMS*, 24 January 2017, https://www.scoutcms.com/news-and-views/5-examples-of-dangerous-counterfeit-products . (Accessed 22 November 2022)
- Groot JD and Brook C, "IP Theft: Definition and Examples" (*Digital Guardian* December 16, 2021) <https://digitalguardian.com/blog/ip-theft-definition-and-examples > (Accessed 22 November 2022)
- "Intellectual Theft: Everything You Need To Know" (*UpCounsel* October 27, 2020) <https://www.upcounsel.com/intellectual-theft > (Accessed November 10, 2022)
- "What Is IP Theft and How to Prevent It from Happening" (*Spirion* July 21, 2022) <https://www.spirion.com/blog/what-is-ip-theft-and-how-to-prevent-it-from-happening/ > (Accessed November 10, 2022)
- "Understanding Malicious Insider Threat Examples to Avoid an Insider Attack" (*Spirion* November 15, 2021) <https://www.spirion.com/blog/malicious-insider-threat-examples /> (Accessed November 10, 2022)
- "Former Employee of Medical Packaging Company Charged with Sabotaging Electronic Shipping Records "(*The United States Department of Justice*April 16, 2020) <https://www.justice.gov/usao-ndga/pr/former-employee-medical-packaging-company-allegedly-sabotages-electronic-shipping >(Accessed November 10, 2022)
- "PCT – The International Patent System." *WIPO*, https://www.wipo.int/pct/en/. (Accessed 22 November 2022)

- Zyl CV, "Luxembourg: What Is Intellectual Property 'Theft' And How To Avoid It?" (*Mondaq* October 1, 2020) <https://www.mondaq.com/trademark/990102/what-is-intellectual-property-39theft39-and-how-to-avoid-it > (Accessed November 10, 2022).
- "What Is Intellectual Property (IP) Theft?" (*Code42* November 9, 2022) <https://www.code42.com/blog/what-is-intellectual-property-theft/ > (Accessed November 10, 2022).