INVESTIGATION · BUSINESS AND CORPORATE INVESTIGATION

Intellectual Property Investigations

Ideas, designs, brands and confidential know-how are among a business's most valuable assets, and among the easiest to take. This article explains the main kinds of intellectual property investigation, how evidence is gathered and the legal tools that support it.

ModQu research article · 1,034 words · 11 references (APA 7th edition)

For many businesses, the most valuable assets cannot be touched. Patents protect inventions, trademarks protect brands, copyright protects software, text and images, design rights protect the appearance of products, and trade secrets protect confidential know-how such as formulas, source code and customer data. Applications for these rights run into the millions each year worldwide (World Intellectual Property Organization [WIPO], 2023). Because these assets are intangible, they can be copied or taken without anyone noticing, and the owner often learns of the loss only when a competing product appears. Intellectual property investigations aim to establish whether rights have been infringed or misappropriated, by whom and to what extent, and to gather evidence that will support legal action.

Types of investigation

The investigation depends on the right involved, since each protects something different and is infringed in different ways.

What is investigated for each type of right

The right involved determines what must be proved

	Typical infringement	Key evidence
Patent	Making or selling a product that uses the claimed invention	Product samples, technical analysis, sales records
Trademark	Using the same or a confusingly similar mark	Test purchases, listings, evidence of confusion
Copyright	Copying software, content or designs	Side-by-side comparison, access, timing
Design	Copying a product's appearance	Product comparison, dates of first marketing
Trade secret	Taking or using confidential information	Access logs, device forensics, timing of departure

Based on the TRIPS Agreement (1994), Directive (EU) 2016/943 and Defend Trade Secrets Act (2016) ModQu.com

Figure 1. Each type of intellectual property right is infringed in a different way, so each investigation looks for different evidence. Diagram by ModQu.

Infringement investigations look outward at competitors and others who may be using protected inventions, brands, content or designs. They typically involve buying and analysing the suspect product, establishing when and where it was sold, and identifying the companies responsible. In patent cases, technical experts compare the product with the patent's claims; in copyright cases, investigators look for evidence of copying, such as identical errors or hidden markers in software code, and evidence that the alleged copier had access to the original. Counterfeiting, the most common form of trademark infringement, is discussed in a separate article.

Online infringement of copyright and trademarks is often handled through notice-and-takedown procedures. In the United States, the Digital Millennium Copyright Act (1998) protects online service providers from liability for content uploaded by users if they remove infringing material promptly when notified. Investigators gather and document the evidence needed for these notices and identify repeat infringers.

Trade secret investigations usually look inward, at employees, contractors and partners who had access to confidential information. They are among the most common and most sensitive kinds of intellectual property investigation.

Investigating trade secret theft

Trade secrets are most often taken by people the owner trusted. An analysis of trade secret cases in United States federal courts found that in most cases the alleged misappropriator was someone the owner knew, usually an employee or a business partner (Almeling et al., 2010). Research on insider threats describes a common pattern: an employee who has decided to leave, often to join a competitor or start a business, copies files in the weeks before departure (Cappelli et al., 2012).

Investigations therefore focus on what departing employees accessed and copied. Forensic examination of laptops, email accounts and cloud storage can show bulk downloads, files copied to removable drives or personal accounts, and attempts to delete evidence. Timing is often the most telling evidence: a large download the evening before a resignation, or access to files unrelated to the employee's current work. In *Waymo LLC v. Uber Technologies, Inc.* (2018), the plaintiff alleged that a former engineer had downloaded about 14,000 confidential files before leaving to found a company that Uber then acquired; the case settled during trial, with Uber agreeing to give Waymo equity and to avoid using its confidential technology.

Not all trade secret theft is by insiders. State-sponsored and criminal hacking groups target intellectual property, and a widely cited report by a security firm linked one group to the theft of large amounts of data from many organisations over several years (Mandiant, 2013). Such cases combine intellectual property investigation with cyber incident response.

Proving that information was taken is only part of the task. The owner must also show that the information qualifies as a trade secret, which means identifying it precisely rather than claiming everything the employee saw, and must often show that it was used or disclosed. Investigators therefore look for evidence in the new employer's products, documents and development timelines: a competing product developed unusually quickly, internal documents with the same structure or errors as the owner's, or files with the owner's metadata on the new employer's systems. Innocent explanations must be tested too. Experienced employees are entitled to use their general skill and knowledge in a new job, and the line between that and confidential information is one of the most contested issues in these cases.

Legal tools

The law provides specific remedies to help owners gather evidence and stop misuse. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement, 1994) requires members to protect undisclosed information and to provide effective enforcement procedures. In the United States, the Defend Trade Secrets Act of 2016 created a federal civil claim for trade secret misappropriation and, in extraordinary circumstances, allows courts to order the seizure of property to prevent the spread of a secret. In the European Union, the Trade Secrets Directive (Directive (EU) 2016/943, 2016) harmonised the definition of a trade secret and the remedies available.

Courts in England and Wales can grant search orders, first recognised in *Anton Piller KG v Manufacturing Processes Ltd* (1976), which allow the claimant's lawyers to enter premises and secure evidence before it can be destroyed, and disclosure orders under *Norwich Pharmacal Co v Customs and Excise Commissioners* (1974), which require third parties to identify wrongdoers. These orders are often sought without notice, so the evidence supporting them must be strong and fairly presented.

Good practice

Intellectual property investigations succeed when owners have done the groundwork before a problem arises. Rights must be registered where they will be enforced, and trade secrets must be identified and protected by reasonable measures, since the law protects only information that its owner has taken steps to keep secret. Access to sensitive information should be limited and logged, so that there is a record to examine if something goes wrong. Exit procedures for departing employees should include the return of devices and reminders of confidentiality obligations.

When an investigation begins, evidence should be preserved before suspects are alerted, devices should be examined by qualified forensic specialists, and privacy and employment law must be respected. Above all, the investigation should establish what was actually taken or copied and whether it was used, since remedies depend on proof of both.

References

Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

Almeling, D. S., Snyder, D. W., Sapoznikow, M., McCollum, W. E., & Weader, J. (2010). A statistical analysis of trade secret litigation in federal courts. *Gonzaga Law Review, 45*(2), 291–334.

Anton Piller KG v Manufacturing Processes Ltd [1976] Ch 55 (CA).

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Addison-Wesley.

Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376.

Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

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). *Official Journal of the European Union, L 157*, 1–18.

Mandiant. (2013). *APT1: Exposing one of China's cyber espionage units*.

Norwich Pharmacal Co v Customs and Excise Commissioners [1974] AC 133 (HL).

Waymo LLC v. Uber Technologies, Inc., No. 3:17-cv-00939-WHA (N.D. Cal. 2018).

World Intellectual Property Organization. (2023). *World intellectual property indicators 2023*.