DOI: http://dx.doi.org/10.18860/j.v15i2.28422

THE LEGALITY OF REVERSE ENGINEERING AND THE PROTECTION OF TRADE SECRETS IN THE SOFTWARE INDUSTRY

Naeem AllahRakha
Tashkent State University of Law, Uzbekistan
Email: chaudharynaeem133@gmail.com

Received: October 11, 2024; Reviewed: October 17, 2024; Accepted: December 17, 2024; Published: December 31, 2024

Abstract

This article explores the legality of reverse engineering and the protection of trade secrets in the software industry. The study aims to provide a comprehensive understanding of the legal framework governing these issues and their implications for software developers and companies. Through a qualitative research methodology employing a doctrinal approach, the study examines relevant legal documents and scholarly articles. The findings suggest that while reverse engineering is generally legal, limitations and exceptions exist to protect trade secrets. The study highlights the importance of implementing effective legal and practical measures to safeguard valuable information in the software industry. Recommendations include the use of licensing agreements, confidentiality agreements, and technological protection measures. This research emphasizes the importance of balancing innovation through reverse

engineering with the protection of intellectual property rights, while also addressing broader implications for the software industry. This article contributes by providing legal and practical guidance for software developers and companies in navigating the challenges between innovation through reverse engineering and the protection of trade secrets.

Artikel ini membahas legalitas rekayasa balik (reverse engineering) dan perlindungan rahasia dagang dalam industri perangkat lunak. Penelitian ini bertujuan memberikan pemahaman yang komprehensif mengenai kerangka hukum yang mengatur isu-isu tersebut serta implikasinya bagi pengembang perangkat lunak dan perusahaan. Melalui metodologi penelitian kualitatif dengan pendekatan doktrinal, penelitian ini menganalisis dokumen hukum yang relevan dan artikel ilmiah. Temuan menunjukkan bahwa meskipun rekayasa balik umumnya legal, terdapat batasan dan pengecualian untuk melindungi rahasia dagang. Penelitian ini menekankan pentingnya penerapan langkah-langkah hukum dan praktis yang efektif untuk melindungi informasi berharga dalam industri perangkat lunak. Rekomendasi mencakup penggunaan perjanjian lisensi, perjanjian kerahasiaan, dan langkah-langkah perlindungan teknologi. Penelitian ini menyoroti pentingnya menyeimbangkan inovasi melalui rekayasa balik dengan perlindungan hak kekayaan intelektual, serta membahas implikasi yang lebih luas bagi industri perangkat lunak. Artikel ini berkontribusi dalam memberikan panduan hukum dan praktis bagi pengembang perangkat lunak dan perusahaan dalam menavigasi tantangan antara inovasi melalui rekayasa balik dan perlindungan rahasia dagang.

Keywords: *reverse engineering, trade secrets, legal frameworks, TRIPS, WIPO.*

Introduction

Reverse engineering involves dissecting and analyzing a device to comprehend its functioning, as illustrated by dismantling an alarm clock to understand its mechanisms. If you aim to devise a personalized coffee maker, examining existing models through reverse engineering can provide crucial insights. This entails disassembling the hardware to thoroughly grasp its operational principles. Through this process, you can discern the constituent parts required for your customized coffee maker and explore various configurations to meet your specifications. Reverse engineering facilitates a comprehensive understanding of a device's inner workings, unveiling its original engineering rationale, identifying flaws, enabling repairs, and offering insights into products inaccessible physically.[1]

Reverse engineering, as defined by the US Supreme Court in Kewanee Oil Co. v. Bicron Corp. (1974), involves the process of deconstructing a known product to understand its design or functionality. It is a method commonly employed in various fields such as machine development and software maintenance. While it can be beneficial for innovation, there are risks involved, including potential exploitation by competitors to replicate products or identify vulnerabilities for malicious purposes, particularly in software. Legally, reverse engineering is generally permissible, recognized as a legitimate means to uncover trade secrets under trade secret law. However, it does not serve as a defense in patent law, as patent owners maintain exclusive rights over their inventions.[2]

It involves several key steps. Firts is prescreening, where the target for reverse engineering is identified and its parameters are understood. The next step is research, which is fundamental for gathering relevant information about the target whether it's hardware, software, or a process. Following this is the

[1] Kienle, H. M., & Müller, H. A. (2010). The Tools Perspective on Software Reverse Engineering: Requirements, Construction, and Evaluation. *Advances in Computers* (Vol. 79, pp. 189-290). https://doi.org/10.1016/S0065-2458(10)79005-7.

[2] Davidson, S. J. (1989). Reverse engineering and the development of compatible and competitive products under United States law. *Santa Clara High Tech. L.J.*, *5*, 399. Retrieved from http://digitalcommons.law.scu.edu/chtlj/vol5/iss2/7.

disassembly phase, where physical objects are taken apart or source code is deconstructed. In the analysis and evaluate stage, engineers meticulously examine each component, documenting flaws and proposing design changes. Reassembly involves reconstructing the product methodically, ensuring accuracy by comparing with the original.[3] Finally, in the creation phase, engineers implement improvements or begin work on a new version using the insights gained during the reverse engineering process. This structured approach ensures a thorough understanding and potentially leads to innovation.[4]

Reverse engineering is a versatile practice applicable to physical objects, software products, and processes alike. When developers lack access to original source code, reverse engineering enables them to reconstruct it by analyzing the end product. It becomes indispensable when portions of source code are lost in legacy systems, aiding in identifying errors or malicious code for subsequent updates. Similarly, when dealing with discontinued products, engineers can dismantle them to recreate blueprints for replication. While reverse engineering processes may be more intricate, it involves mapping relevant information using tools like data flow diagrams and structure charts to understand how an end result is achieved.[5]

In the mid-1980s, Phoenix Technologies Ltd., based in San Jose, undertook a notable instance of reverse-engineering by creating a compatible BIOS for PCs, mimicking IBM's proprietary BIOS. Employing a "clean room" methodology, one team meticulously documented IBM's BIOS functionality without referencing its code, while a separate team, devoid of prior exposure to

[3] AllahRakha, N. (2024). Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds. *Lex Scientia Law Review*, 8(1), 405-432. https://doi.org/10.15294/lslr.v8i1.2081.

[4] Snider, M., Teegavarapu, S., Hesser, D. S., & Summers, J. D. (2006). Augmenting Tools for Reverse Engineering Methods. *Proceedings of the ASME 2006 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference* (pp. 371-380). Philadelphia, Pennsylvania, USA: ASME. https://doi.org/10.1115/DETC2006-99676.

[5] Geng, Z., & Bidanda, B. (2017). Review of reverse engineering systems – current state of the art. *Virtual and Physical Prototyping, 12*(2), 161-172. https://doi.org/10.1080/17452759.2017.1302787.

IBM's BIOS, developed a new BIOS based solely on the functional specifications provided. Despite differences in code, the resulting Phoenix BIOS functioned identically to IBM's, allowing Phoenix to supply it to manufacturers for IBM-compatible PCs legally. Similarly, companies such as Cyrix Corp. and Advanced Micro Devices Inc. have reverse-engineered Intel microprocessors, enabling the production of cost-effective Intel-compatible chips. These cases highlight how reverse engineering has been used to foster competition and innovation in the technology sector.[6]

Reverse-engineering, while legal, is increasingly facing challenges due to legal constraints imposed by companies and legislation like the Digital Millennium Copyright Act (DMCA). For example, companies like Digital: Convergence Corp.'s CueCat have been found to exploit reverse-engineering to track user habits without public disclosure. Additioonally, shrink-wrap licenses pose significant threats to reverse engineering, as they often inhabit investigations into software functionalities and security flaws. While such licenses may permit reverse engineering for purposes like ensuring compatibility, they frequently restrict probing software for its intended functionality or scientific exploration. This practice has been likened to owning a car but being forbidden to inspect its mechanics.[7]

The term "monopoly" is often used to describe instances where there is a single seller of a good in a market. In the United States, antitrust legislation serves to prevent monopolies, which can hinder competition and harm consumers. The Sherman Antitrust Act of 1890 targeted trusts, precursor organizations to monopolies, breaking up giants like Standard Oil and American Tobacco. The Clayton Antitrust Act of 1914 further regulated mergers and business practices, supported by the Federal Trade Commission

[6] Chiriţă, A.-P., Borş, A.-M., Rădoi, R.-I., Dumitrescu, I.-C., & Popescu, A.-M. C. (2023). Leveraging Additive Manufacturing and Reverse Engineering for Circular Economy-Driven Remanufacturing of Hydraulic Drive System Components. *Applied Sciences*, 13(22), 12200. https://doi.org/10.3390/app132212200.

[7] Samuelson, P., & Scotchmer, S. (2002). The Law and Economics of Reverse Engineering. *The Yale Law Journal*, *111*(7), 1575–1663. https://doi.org/10.2307/797533.

Act, establishing the FTC to enforce these laws. Notable was the 1982 dissolution of AT&T's telephone monopoly. Microsoft faced antitrust allegations in 1994 for leveraging its dominance in personal computer operating systems to stifle competition. While initially facing breakup, Microsoft ultimately retained its structure after an appeal.[8]

Confidentiality refers to the safeguarding of sensitive information among designated parties. In accordance with legal standards, a trade secret must have commercial value due to its secrecy and require reasonable measures to maintain confidentiality. To ensure confidentiality within a corporate framework, a structured approach is imperative. This includes labeling documents appropriately, limiting access, implementing secure IT systems, and establishing a comprehensive data protection policy. While confidentiality is crucial for individuals with secretive affiliations, it extends beyond illicit activities, safeguarding various aspects such as reputation and employment opportunities. It's vital to recognize that confidential information, especially trade secrets, holds significant business value and necessitates protection against misuse or unauthorized disclosure, thereby contributing to the integrity and success of an organization.[9]

The ISO/IEC 27000:2018 standard on information technology security techniques outlines the fundamentals of Information Security Management Systems (ISMS). It provides a comprehensive framework for safeguarding sensitive data. The standard defines confidentiality as the assurance that information remains inaccessible and undisclosed to unauthorized individuals, entities, or processes (Clause 3.10). This principle underlines the protection of sensitive information from breaches or unauthorized access. The standard serves as a universal guideline applicable to organizations of all sizes and

[8] Page, Amy C. (1994) "Microsoft: A Case Study in International Competitiveness, High Technology, and the Future of Antitrust Law," *Federal Communications Law Journal*: Vol. 47: Iss. 1, Article 9. Available at: https://www.repository.law.indiana.edu/fclj/vol47/iss1/9.
[9] Bos, J. (2020). Confidentiality. In J. Bos (Ed.), *Research Ethics for Students in the Social Sciences*. Springer. https://doi.org/10.1007/978-3-030-48415-6_7.

types, including commercial enterprises, government agencies, and not-for-profit organizations.[10]

Intellectual property (IP) encompasses creations of the mind, ranging from inventions to artistic works, which are protected by patents, copyrights, trademarks, and other mechanisms. Patents grant exclusive rights to inventors, enabling them to control the use of their inventions in exchange for public disclosure. Copyrights safeguard literary and artistic works, while trademarks distinguish the goods or services of one entity from those of another. Industrial designs protect the aesthetic aspects of products, and geographical indications identify goods originating from specific locations with unique qualities.[11]

Trade secrets safeguarding a company's intellectual property, often without the explicit realization of their legal protection. Notable examples like the Coca Cola formula and software source codes highlight their significance. Unlike patents, trade secrets endure indefinitely, contingent upon the maintenance of confidentiality agreements. While mere ideas are generally not eligible, specific ideas can qualify if they demonstrate novelty and tangible form. These proprietary practices and processes confer a competitive edge, characterized by secrecy, economic advantage, and active safeguarding. However, information readily discernible through product dissection isn't considered a trade secret. Typically, trade secrets are corporate assets, even if originating from employee contributions, emphasizing their organizational ownership.[12]

---

[10] Kamil, Y., Lund, S., & Islam, M.S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and E-Business Management*, 21, 699–722. https://doi.org/10.1007/s10257-023-00646-y.

[11] Saha, C. N., & Bhattacharya, S. (2011). Intellectual property rights: An overview and implications in pharmaceutical industry. *Journal of Advanced Pharmaceutical Technology & Research*, 2(2), 88–93. https://doi.org/10.4103/2231-4040.82952.

[12] Irgens-Jensen, H. (2023). Departing employees, confidentiality clauses and European trade secret protection. *IIC, International Review of Intellectual Property and Competition Law, 54*(4), 495–526. https://doi.org/10.1007/s40319-023-01311-0

This study aims to investigate the legality of reverse engineering and the extent to which trade secrets are protected in the software industry. The central research question is: How do legal frameworks and industry practices balance the need for innovation through reverse engineering with the protection of intellectual property rights in the form of trade secrets? The hypothesis is that while reverse engineering is generally permitted under certain conditions, there are limitations and exceptions in place to safeguard trade secrets and prevent unfair competition. By examining relevant legal documents, case studies, and scholarly articles, this research seeks to provide a comprehensive understanding of the current landscape and offer recommendations for software developers and companies navigating this complex issue.

Research Methods

This study employs a qualitative research methodology to investigate the legality of reverse engineering and the protection of trade secrets in the software industry. The research methods were developed through a comprehensive literature review, examining relevant legal documents, case studies, and scholarly articles to gain a deep understanding of the subject matter. The data collection process involved a doctrinal research approach, which entailed the systematic analysis of legal documents, including statutes, regulations, and court decisions related to reverse engineering and trade secret protection. This approach allowed for a thorough examination of the legal framework governing these issues in the software industry. The study utilized existing data from scholarly articles, industry reports, and case studies to form new insights and perspectives on the topic.[13]

To analyze the collected data, the study employed a grounded theory approach. This involved the careful organization and categorization of the information gathered through the research process. The data was then

[13] Al Fatih, S. (2023). *The Development of Legal Research Methods in Indonesia*. UMM Press.

systematically studied to identify patterns, themes, and relationships between different aspects of reverse engineering and trade secret protection in the software industry. This iterative process of data analysis allowed for the development of a comprehensive understanding of the legal landscape and its implications for software developers and companies. The tools and materials used in this study primarily consisted of legal databases, such as LexisNexis and Westlaw, which provided access to a wide range of legal documents and case law. The scholarly databases, including Google Scholar and JSTOR, were utilized to access relevant academic literature on the topic. Other resources, such as industry reports and whitepapers, were also consulted to gain insights into the practical implications of reverse engineering and trade secret protection in the software industry.

The rationale behind this methodology is to provide a comprehensive and rigorous analysis of the legality of reverse engineering and the protection of trade secrets in the software industry. By employing a qualitative research methodology, a doctrinal research approach, and a grounded theory analysis, this study aims to contribute to the existing body of knowledge on the subject matter and provide valuable insights for software developers, companies, and policymakers. The systematic and thorough examination of legal documents, case studies, and scholarly articles ensures that the findings of this study are valid, relevant, and grounded in a solid understanding of the legal framework governing reverse engineering and trade secret protection in the software industry.

Discussion

The Legality of Reverse Engineering and The Protection of Trade Secrets in The Software Industry

This study aimed to explore the various methods that trade secret holders can employ to protect their valuable information from reverse engineering activities. The findings suggest that there are several effective strategies available to safeguard trade secrets, each with its own advantages and

limitations. While information and knowledge diffusion and free competition are considered the rule, and intellectual property protection the exception, trade secret regulation is no exception. Since the protection of trade secrets is not conditional on disclosure or a quid pro quo, the holder's rights are more limited compared to other forms of intellectual property protection. Trade secret holders must therefore rely on a combination of legal and practical measures to safeguard their valuable information from reverse engineering activities.[14]

Licensing agreements have emerged as a straightforward approach to mitigating the threat of reverse engineering. By granting licenses, trade secret holders can regulate the entry of new competitors into the market while recovering their research and development expenses through licensing revenues. These agreements also prevent licensees from engaging in destructive pricing practices that could harm the market. Licensing agreements offer competitors an opportunity to access the same secret information and economic benefits as reverse engineering, without the need to invest significant resources in the reverse engineering process. As long as reverse engineering is legally permitted, trade secret holders are likely to offer licenses on favorable terms to deter reverse engineering.[15]

Confidentiality agreements are another effective means of protecting trade secrets across all stages of business relations. Reverse engineers may even be required to sign such agreements with the enterprise or individual for whom they provide their services. For example, the freelancing platform CadCrowd imposes strict confidentiality rules on engineers through its Terms of Service. These rules require engineers to maintain the confidentiality of information, refrain from unauthorized copying or use, obtain prior written consent before

[14] LaRoque, S. J. (2017). Reverse Engineering and Trade Secrets in the Post-Alice World. *Kansas Law Review*, 66, 427-457. Retrieved from https://kuscholarworks.ku.edu/bitstream/handle/1808/25704/10_LaRoque_Final.pdf?sequence=1&isAllowed=y.

[15] Mauk, J. E. (2001). The Slippery Slope of Secrecy: Why Patent Law Preempts Reverse-Engineering Clauses in Shrink-Wrap Licenses. *William & Mary Law Review*, 43(2), 819. https://scholarship.law.wm.edu/wmlr/vol43/iss2/7.

disclosing information, and protect the information from unauthorized access[16]. An indirect method to counterbalance reverse engineering is increasing brand awareness through marketing campaigns. By promoting a brand, innovative products can maintain their market share and remain distinguishable from similar products that may enter the market later. The Coca-Cola brand, which incorporates trade secrets in its manufacturing recipe, exemplifies this approach by achieving international recognition despite competition from similar products.[17]

Trade secret holders can implement protection measures against reverse engineering during the design and manufacturing stages of their products. These measures include using sealing systems or construction materials that degrade or break down during disassembly, thereby making reverse engineering difficult or impossible. Manufacturers can also employ techniques such as encapsulating hardware components, mislabeling or marking components to mislead potential reverse engineers, and adding 'locks' on product components or within software programs. In addition to these technological measures, some state legislators have enacted regulations to penalize the illegal use of trade secrets and anti-competitive practices. Such practices may involve using information obtained through reverse engineering to create slavish imitations of existing products. Several U.S. states have implemented rules prohibiting the creation of molds for reverse engineering purposes. These regulations forbid using molds to manufacture identical products that compete directly with the original molded product.[18]

The European Union's Directive 2016/943 considers the production, offering, or placing on the market of infringing goods, as well as their

---

[16] AllahRakha, N. (2024). Global Perspectives on Cybercrime Legislation. *Journal of Infrastructure, Policy and Development*, 8(10), 6007. https://doi.org/ 10.24294/jipd.v8i10.6007.

[17] Mahfuzzah, Z., Saidin, S., Ginting, B., & Devi, T. K. (2024). Non-disclosure Agreements (NDA) as a Legal Protection on Trade Secrets in Work Agreements in Indonesia. *KnowledgeE*, *8*(21). https://doi.org/10.18502/kss.v8i21.14768.

[18] Radauer, A., Searle, N., & Bader, M. A. (2023). The possibilities and limits of trade secrets to protect data shared between firms in agricultural and food sectors. *World Patent Information, 73*, 102183. https://doi.org/10.1016/j.wpi.2023.102183.

importation, export, or storage for those purposes, to be an unlawful use of a trade secret when the person carrying out such activities knew or should have known that the trade secret was used unlawfully. At the EU level, trade secret holders have the right to apply to competent courts for the enforcement of measures, procedures, and remedies provided by law to prevent, restrain, or obtain redress for the unlawful acquisition, use, or disclosure of their trade secrets. Unlike patents, where disclosed information becomes part of the public domain (prior art), trade secrets are not made public and therefore do not offer 'defensive' protection to the holder. This means that if a manufacturing process is protected as a trade secret, others may still obtain a patent for the same technological process if they independently developed or discovered the information.[19]

The World Intellectual Property Organization (WIPO) affirms that a trade secret owner cannot prevent others from using the same technical or commercial information if it was independently acquired or developed through legitimate means such as research and development, reverse engineering, or marketing analysis. In recent developments, the Fédération Internationale de l'Automobile (FIA) revised its technical regulations for Formula 1, prohibiting reverse engineering regarding the design of rival competitors. The new regulation prevents competitors from designing their Listed Team Components (LTC) based on reverse engineering of another competitor's LTC. However, the FIA does not entirely prohibit reverse engineering—it only restricts reverse engineering that specifically targets competitor designs. For instance, creating digital replicas or digital twins of rival cars with improved performance appears to remain permissible.[20]

[19] Hoeren, T. (2020). *The New EU Directive on the Protection of Trade Secrets and Its Implementation*. Springer Nature Singapore Pte Ltd.
[20] Gerard-Reimer, C. C. (2021). Race Cartels: How Constructor Collaboration Is Curbing Innovation in Formula 1. *Vanderbilt Journal of Entertainment and Technology Law*, 23, 855. https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss4/4.

The Legality of Reverse Engineering and Trade Secret Protection in an International Perspective

The commercial Secrets refer to confidential technical and economic data not publicly known, possessing potential economic value for competitors, with practical applications, and safeguarded by their proprietor.[21] The Law of the Republic of Uzbekistan on Trade Secrets, enacted on September 12, 2014, defines a trade secret as information with commercial value in various fields, inaccessible to third parties with measures taken to maintain its confidentiality (Article 3). The criteria for a trade secret, emphasizing its commercial value, non-public status, confidentiality measures, and absence of state or legally protected secrets (Article 4). The rights of trade secret owners, including the establishment of secrecy protocols, control over access, and recourse against unauthorized disclosure or use (Article 6). Furthermore, the trade secrets remain protected until their confidentiality is compromised (Article 7).[22]

The TRIPS Agreement establishes fundamental standards for safeguarding various forms of intellectual property. Article 39 of TRIPS outlines obligations concerning undisclosed information and data submitted to governments. It mandates member states to protect confidential information from unfair competition by ensuring it remains undisclosed, acquired, or used without consent. This protection applies when the information meets specific criteria of secrecy, commercial value, and reasonable steps to maintain confidentiality. Additionally, TRIPS requires member states to safeguard undisclosed test data or other submissions for pharmaceutical or agricultural chemical products, recognizing the effort involved in generating such data.

[21] Verma, S. K. (2002). LEGAL PROTECTION OF TRADE SECRETS AND CONFIDENTIAL INFORMATION. *Journal of the Indian Law Institute*, *44*(3), 336–353. http://www.jstor.org/stable/43951824.
[22] Republic of Uzbekistan. (2014). Law on Trade Secrets, No. LRU-374. Retrieved from https://lex.uz/ru/docs/6642218.

Disclosure is permitted only when necessary for public interest or if adequate protections against unfair commercial use are implemented.[23]

The Uniform Trade Secrets Act (UTSA), established by the Uniform Law Commission in 1979 and updated in 1985, aims to standardize trade secret laws across the United States, facilitating consistency for businesses operating in multiple states. Currently adopted by 48 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, the UTSA defines a trade secret as confidential information with economic value that is not generally known or readily accessible, and reasonable efforts are made to maintain its secrecy (Section 1.4). The act provides injunctive relief for misappropriation and allows for damages, including actual loss and unjust enrichment, with potential for doubling damages in cases of willful misconduct (Section 2, 3). It ensures the preservation of secrecy during legal proceedings, allowing courts to implement measures like sealing records to safeguard trade secrets (Section 5).[24]

The legality of reverse engineering has been firmly established through both case law and statutory provisions. The Supreme Court of the United States has consistently upheld the right to reverse engineer products as a legitimate means of acquiring knowledge and fostering innovation. In the seminal case of Kewanee Oil Co. v. Bicron Corp., the Supreme Court unequivocally stated that trade secret laws do not offer protection against the discovery of information through fair and honest means. Such means include independent invention, accidental disclosure, and the practice of reverse engineering. The Court's decision highlights the importance of allowing individuals and businesses to learn from and build upon existing technologies, provided the process of acquiring such knowledge is conducted lawfully. This statutory recognition,

[23] World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS): Part II — Standards concerning the availability, scope and use of Intellectual Property Rights, Sections 7 and 8. Retrieved from https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm.

[24] Nashkova, S. (2023). Defining Trade Secrets in the United States: Past and Present Challenges – A Way Forward?. *IIC, 54*(5), 634–672. https://doi.org/10.1007/s40319-023-01310-1.

combined with the Supreme Court's rulings, creates a clear legal framework in the United States that supports reverse engineering as a vital tool for technological advancement and competition.[25]

Point (14) of Directive (EU) 2016/943 emphasizes the need for a unified definition of trade secrets, encompassing know-how, business, and technological information, provided there's a genuine interest in confidentiality and an expectation of its preservation. Such information must hold commercial value, either current or potential, with its misuse posing a threat to the lawful controller's scientific, technical, financial, or competitive interests. The definition excludes trivial data and skills acquired by employees in their normal duties, as well as information known or accessible within relevant circles. This directive aims to safeguard valuable proprietary information while allowing for legitimate business practices and employee rights within the European Union.[26]

It focuses on safeguarding undisclosed know-how and business information, commonly referred to as trade secrets, from unlawful acquisition, usage, and disclosure. A 'trade secret' is defined as information meeting specific criteria: it must be kept confidential within relevant circles, possess commercial value due to its secrecy, and have been subject to reasonable confidentiality measures by the rightful owner. A 'trade secret holder' is any individual or entity legitimately controlling such information, while an 'infringer' pertains to anyone unlawfully obtaining, utilizing, or revealing a trade secret. Additionally, 'infringing goods' are products benefiting significantly from unlawfully acquired trade secrets in their design, characteristics, production process, or marketing strategies (Article 2).[27]

---

[25] Sandeen, S. K. (2008). Kewanee revisited: Returning to first principles of intellectual property law to determine the issue of federal preemption. *Intellectual Property Law Review*, 12, 299. Retrieved from http://scholarship.law.marquette.edu/iplr/vol12/iss2/3.

[26] Arcidiacono, D. (2016). The Trade Secrets Directive in the International Legal Framework. *European Papers*, 1(3), 1073-1085. https://doi.org/10.15166/2499-8249/83.

[27] Mylly, U. M. (2023). Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information. *IIC, 54*(8), 1013–1043. https://doi.org/10.1007/s40319-023-01328-5.

Commission Regulation (EU) No 316/2014, enacted on March 21, 2014, delineates key definitions pertinent to technology transfer agreements within the European Union. Under this regulation, 'technology rights' encompass patents, utility models, design rights, semiconductor product topographies, supplementary protection certificates, plant breeder's certificates, and software copyrights. A 'technology transfer agreement' refers to a licensing agreement or assignment of technology rights between undertakings for the production of contract products, with the assignor retaining some risk. The regulation emphasizes 'know-how' as confidential, significant practical information crucial for product production, requiring secrecy, substantiality, and clear identification. (Article 1). The know-how principle refers to the protection of valuable, confidential, and technical information that provides a competitive advantage to its holder. It is recognized as a form of intellectual property, distinct from patents or trademarks, and is often transferred through licensing agreements or protected as a trade secret. For example, a company's proprietary manufacturing process, which is not patented but is kept confidential, would be considered know-how.[28]

Undisclosed business information, also known as confidential information or trade secrets, is a form of intellectual property that holds immense value for companies and organizations. Unlike patents, trademarks, or copyrights, which require formal registration processes and involve associated costs, undisclosed business information can be protected indefinitely without any official procedures, as long as the information remains secret. This makes it an attractive and cost-effective means of safeguarding a company's competitive advantage. The protection of undisclosed business information is rooted in the principle that such information is a form of property, and as such, it is entitled

[28] Kumar, R. (2014). Technology Transfer Agreements within the European Union: An Analysis of Block Exemption Regulation. *Journal of Intellectual Property Rights*, 19(3), 229-233. https://nopr.niscpr.res.in/bitstream/123456789/28930/1/JIPR%2019%283%29%20229-233.pdf.

to legal protection under property rights laws.[29] This notion is reinforced by international legal frameworks, such as Article 1 Protocol 1 of the European Convention on Human Rights, which recognizes the right to peaceful enjoyment of one's possessions. The legal protection afforded to undisclosed business information allows companies to maintain their competitive edge by preventing the unauthorized disclosure, use, or acquisition of their valuable confidential information.[30]

In the copyright law, which safeguards the expression of ideas rather than the ideas themselves, the concept of reverse engineering has been a topic of discussion, particularly in the context of computer programs. The Court of Justice of the European Union (CJEU) provided clarity on this matter in the landmark case of SAS Institute v. World Programming Ltd (C-406/10). The case revolved around an alleged infringement of copyright on computer programs and manuals related to an IT database system, brought forth by SAS Institute. In its ruling, the CJEU emphasized that the functionality of a computer program and the programming language or format of data files used in a computer program do not constitute a form of expression and thus are not protected by copyright. This decision effectively allows for the reverse engineering of computer programs, as long as the process does not infringe upon the specific expression of the original program.[31]

In common law, the legality of reverse engineering hinges on a fundamental condition: the ownership of the product being "disassembled." This principle was firmly established in the British court case of Mars UK Ltd v.

---

[29] Yeh, B. T. (2016). Protection of Trade Secrets: Overview of Current Law and Legislation (CRS Report No. R43714). Congressional Research Service. https://sgp.fas.org/crs/secrecy/R43714.pdf.

[30] Sengar, D. S. (2011). PROTECTION OF TRADE SECRETS AND UNDISCLOSED INFORMATION: LAW AND LITIGATION. *Journal of the Indian Law Institute*, *53*(2), 254–274. http://www.jstor.org/stable/43953505.

[31] Schuldt, L. (2023). *EU Copyright and Trade Mark Law: a unifying lens for the protection of Fashion Designs?* Analysis and research into a better understanding of the concepts of originality and distinctiveness. Retrieved from https://www.diva-portal.org/smash/get/diva2:1776959/FULLTEXT01.pdf.

Teknowledge Ltd in 2000. The court's ruling emphasized that when an individual or entity lawfully acquires ownership of a product, they are bestowed with the full rights and privileges associated with that ownership. Among these rights is the entitlement to dismantle the product to gain an understanding of its inner workings and to share that knowledge with others as they see fit. This decision highlights the common law's recognition of the inherent rights of property owners to explore, study, and learn from the products they rightfully possess.[32]

In the European Union, the legal framework surrounding reverse engineering takes a slightly different approach compared to the common law's emphasis on ownership. The EU's Directive 2016/943, which aims to harmonize the protection of trade secrets across member states, establishes the conditions under which reverse engineering is considered lawful. According to Article 3, paragraph (1) (b) of the Directive, the observation, study, disassembly, or testing of a product or object is permitted if the item in question has either been made available to the public or is lawfully in the possession of the person acquiring the information. However, this provision is subject to the absence of any legally valid contractual obligation that limits the acquisition of the trade secret. This means that if an individual or entity is bound by a licensing agreement, such as a software license, that restricts the reverse engineering of the product, they may be prohibited from engaging in such activities.[33]

The Directive strikes a balance between safeguarding the intellectual property rights of software developers and promoting interoperability within the software industry. Article 1, paragraphs (2) and (3) of the Directive, establishes that copyright protection extends to the expression of a computer program in any form. However, the Directive also recognizes the importance of allowing for the decompilation of software under specific circumstances.

[32] Trallero Ocaña, T. (2021). Chapter 6. The internal and external spheres of secrecy and their limitations. In *The Notion of Secrecy* (pp. 467-560). DOI: 10.5771/9783748911975-467.
[33] Birnhack, M. (2013). Reverse engineering informational privacy law. *Yale Journal of Law & Technology, 15*(1). Retrieved from https://digitalcommons.law.yale.edu/yjolt/vol15/iss1/3.

Decompilation, a form of reverse engineering, is permitted when it is carried out with the sole purpose of achieving interoperability between independently created computer programs. This provision enables software developers to analyze and understand the functioning of existing programs to create compatible and interoperable solutions.[34]

Directive 2009/24/CE of the European Union provides a protection of computer programs and addresses the issue of reverse engineering in the form of decompilation. Article 6 of the Directive specifically allows for the reproduction of the object code and its decompilation without the authorization of the rights holder, but only under certain conditions and for the specific purpose of achieving interoperability between independently created software programs. The Directive sets out three key conditions that must be met for decompilation to be permissible.[35]

Firstly, the acts must be performed by the licensee, another person with the right to use a copy of the program, or someone authorized on their behalf. Secondly, the information necessary for interoperability must not have been previously readily available to these individuals. Lastly, the decompilation must be confined to the parts of the original program that are essential for achieving interoperability.

Article 6, paragraph 2(c) of the Directive places restrictions on the use of the information obtained through decompilation. It stipulates that such information cannot be used for developing, producing, or marketing a computer program that is substantially similar in its expression to the original program, or for any other act that infringes upon copyright.[36]

---

[34] Palmer, A. K., & Vinje, T. C. (1992). The EC directive on the legal protection of computer software: New law governing software development. *Duke Journal of Comparative & International Law, 2*(65-87). Retrieved from https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1307&context=djcil.

[35] Mylly, U.-M. (2013). *Intellectual property protection of computer program interfaces and interoperability* (Publications of IPR University Center No. 12). Helsinki, Finland: Oy Nord Print Ab.

[36] Ehrlich, M. A. (1994). Fair Use or Foul Play? The EC Directive on the Legal Protection of Computer Programs and Its Impact on Reverse Engineering. *Pace Law Review, 13*(3), 1003. https://doi.org/10.58948/2331-3528.1420.

Article 5, paragraph (3) of Directive 2009/24/CE introduces another form of reverse engineering that is permitted under European Union law. This provision grants individuals who have the right to use a copy of a computer program the ability to observe, study, or test the functioning of the program without requiring the authorization of the rights holder. The purpose of this provision is to allow users to determine the underlying ideas and principles that form the basis of any element of the program. However, this entitlement is limited to the context of performing acts that the user is already legally entitled to do, such as loading, displaying, running, transmitting, or storing the program. This form of reverse engineering, often referred to as "black-box" analysis, enables users to gain a deeper understanding of how the software functions and the fundamental concepts that underpin its design.[37]

The European Union's Directive 2009/24/EC provides robust protections for users' rights to decompile, copy, analyze, study, or test the operation of a program to identify its underlying ideas and principles. Article 8, paragraph 2 of the Directive explicitly states that contractual clauses that seek to restrict these activities are null and void, emphasizing the importance of allowing users to engage in these forms of reverse engineering. The Court of Justice of the European Union (CJEU) recently reinforced this notion in the case of Top System SA v. Belgian State (C-13/20). The Court ruled that a lawful purchaser of a computer program who wishes to decompile the program to correct errors affecting its operation is not bound by the requirements laid out in Article 6 of the Directive. However, the Court clarified that such decompilation should be limited to the extent necessary for error correction and must comply with any relevant conditions stipulated in the contract with the copyright holder.[38]

---

[37] Shemtov, N. (2017). On reverse engineering and decompilation. *Beyond the Code: Protection of Non-Textual Features of Software*. Oxford Academic. https://doi.org/10.1093/oso/9780198716792.003.0003.

[38] Weston, S. (2017). Improving interoperability by encouraging the sharing of interface specifications. *Law, Innovation and Technology*, 9(1), 78-116. https://doi.org/10.1080/17579961.2017.1302695.

The World Intellectual Property Organization (WIPO), recognizes the importance of protecting valuable confidential information that provides a competitive advantage to businesses. However, WIPO also acknowledges the limitations of trade secret protection and emphasizes that a trade secret owner cannot prevent others from using the same technical or commercial information if they have acquired or developed it independently through their own means. This includes scenarios where the information is obtained through research and development (R&D), reverse engineering, or marketing analysis. WIPO's stance on this matter highlights the delicate balance between safeguarding the rights of trade secret owners and fostering innovation and fair competition in the marketplace. WIPO encourages businesses to invest in their own R&D efforts and engage in legitimate market research.[39]

In the European Union, the legal framework surrounding reverse engineering of computer programs, as outlined in Directive 2009/24/EC, grants users the right to decompile, copy, analyze, study, or test the operation of a program to identify its underlying ideas and principles. Crucially, Article 8, paragraph 2 of the Directive renders any contractual clauses that attempt to restrict these activities null and void, ensuring that users' rights to engage in reverse engineering are protected. The Court of Justice of the European Union (CJEU) recently reinforced this principle in the case of Top System SA v. Belgian State (C-13/20). The Court ruled that a lawful purchaser of a computer program who wishes to decompile the program to correct errors affecting its operation is not obligated to meet the requirements set forth in Article 6 of the Directive.[40]

In the United States, the restriction of reverse engineering through contractual agreements remains controversial and subject to differing

[39] Caplanova, A. (2016). Start-Up Creation: Intellectual property. In *The Smart Eco-Efficient Built Environment* (pp. 105-126). https://doi.org/10.1016/B978-0-08-100546-0.00007-8.
[40] Mancaleoni, A. M., & Poillot, E.. (2021). *National judges and the case law of the Court of Justice of the European Union:* Proceedings of the conference held in Cagliari, 1st June 2018. Università degli Studi Roma Tre, Dipartimento di Giurisprudenza. Retrieved from https://romatrepress.uniroma3.it/wp-content/uploads/2021/01/nati-mape.pdf.

interpretations by the courts. The 1988 case of Vault Corporation v. Quaid Software Limited declared prohibitions on reverse engineering unenforceable, while the 2005 case of Davidson & Associates v. Jung upheld the validity of such restrictions when agreed upon in the terms of use or end-user license agreements. The court in Davidson & Associates v. Jung distinguished the case from Vault, stating that the contractual restrictions did not conflict with federal law or restrict rights provided under it. Restricting the right to reverse engineer through contracts can potentially stifle progress and lead to unfair market conditions, as demonstrated in the Microsoft v. European Commission case. The landmark cases of Sega Enterprises Ltd. v. Accolade Inc. and Sony Computer Entertainment Inc. v. Connectix Corp. shed light on the unique motivations for reverse engineering in the software industry, particularly the need to ensure interoperability between programs and platforms.[41]

Conclusion

The legality of reverse engineering and the protection of trade secrets in the software industry are critical topics that directly impact innovation, competition, and the delicate balance between intellectual property rights and the dissemination of knowledge. This study asserts that while reverse engineering is generally legal, limitations and exceptions exist to protect trade secrets. Throughout this article, several key points have been emphasized. First, the legality of reverse engineering is subject to specific conditions, such as the requirement that the software being reverse-engineered must have been obtained lawfully. Second, trade secret protection is not absolute and does not provide the same level of defensive protection as patents. Third, software developers and companies can mitigate the risks associated with reverse

[41] Chen, Y. (2022). Enforceability of Anti-Reverse Engineering Clauses in Software Licensing Agreements: The Chinese Position and Lessons from the United States and European Union's Laws. *University of Pennsylvania Journal of International Law*, *43*(3), 783-819. Retrieved from https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2052&context=jil.

engineering through strategies such as licensing agreements, confidentiality agreements, and technological protection measures.

A key insight provided by this study is that the legal framework surrounding reverse engineering and trade secret protection is not always clear-cut, with blurred boundaries between legal and illegal practices in certain cases. In light of these findings, this article recommends that software developers and companies take proactive steps to safeguard their trade secrets. These steps include implementing robust licensing and confidentiality agreements and investing in technological protection measures. Future studies could examine the effectiveness of these legal and practical measures in mitigating the risks associated with reverse engineering, as well as the potential unintended consequences of overly restrictive policies. The legality of reverse engineering and the protection of trade secrets in the software industry remain complex and multifaceted issues requiring ongoing attention and adaptation. By understanding the legal framework, adopting effective protective measures, and fostering a culture of innovation and collaboration, software developers and companies can navigate this challenging landscape and continue to drive the industry forward.

References

Arcidiacono, Davide. "The Trade Secrets Directive in the International Legal Framework." *European Papers* 1, no. 3 (2016): 1073-1085. https://doi.org/10.15166/2499-8249/83.

AllahRakha, N. (2024). Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds. *Lex Scientia Law Review*, 8(1), 405-432. https://doi.org/10.15294/lslr.v8i1.2081

AllahRakha, N. (2024). Global Perspectives on Cybercrime Legislation. *Journal of Infrastructure, Policy and Development*, 8(10), 6007. https://doi.org/10.24294/jipd.v8i10.6007

Birnhack, Michael. "Reverse engineering informational privacy law." *Yale Journal of Law & Technology* 15, no. 1 (2013). https://digitalcommons.law.yale.edu/yjolt/vol15/iss1/3.

Bos, Jelle. "*Confidentiality.*" Research Ethics for Students in the Social Sciences, Springer, 2020. https://doi.org/10.1007/978-3-030-48415-6_7.

Caplanova, Anetta. *"Start-Up Creation: Intellectual property."* The Smart Eco-Efficient Built Environment, 105-126, 2016. https://doi.org/10.1016/B978-0-08-100546-0.00007-8.

Chen, Yifan. "Enforceability of Anti-Reverse Engineering Clauses in Software Licensing Agreements: The Chinese Position and Lessons from the United States and European Union's Laws." *University of Pennsylvania Journal of International Law* 43, no. 3 (2022): 783-819. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2052&context=jil.

Chiriță, A.-P., A.-M. Borș, R.-I. Rădoi, I.-C. Dumitrescu, and A.-M. C. Popescu. "Leveraging Additive Manufacturing and Reverse Engineering for Circular Economy-Driven Remanufacturing of Hydraulic Drive System Components." *Applied Sciences* 13, no. 22 (2023): 12200. https://doi.org/10.3390/app132212200.

Davidson, Stephen J. "Reverse engineering and the development of compatible and competitive products under United States law." *Santa Clara High Tech. L.J.* 5 (1989): 399. http://digitalcommons.law.scu.edu/chtlj/vol5/iss2/7.

Ehrlich, Marsha A. "Fair Use or Foul Play? The EC Directive on the Legal Protection of Computer Programs and Its Impact on Reverse Engineering." *Pace Law Review* 13, no. 3 (1994): 1003. https://doi.org/10.58948/2331-3528.1420.

Geng, Zhe, and Bopaya Bidanda. "Review of reverse engineering systems – current state of the art." *Virtual and Physical Prototyping* 12, no. 2 (2017): 161-172. https://doi.org/10.1080/17452759.2017.1302787.

Gerard-Reimer, Corinna C. "Race Cartels: How Constructor Collaboration Is Curbing Innovation in Formula 1." *Vanderbilt Journal of Entertainment and Technology Law* 23 (2021): 855. https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss4/4.

Hoeren, Thomas. *The New EU Directive on the Protection of Trade Secrets and Its Implementation.* Springer Nature Singapore Pte Ltd., 2020.

Irgens-Jensen, Harald. "Departing employees, confidentiality clauses and European trade secret protection." IIC, *International Review of Intellectual Property and Competition Law* 54, no. 4 (2023): 495–526. https://doi.org/10.1007/s40319-023-01311-0.

Kamil, Yousra, Svente Lund, and Mariam Suad Islam. "Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden." *Information Systems and E-Business Management* 21 (2023): 699–722. https://doi.org/10.1007/s10257-023-00646-y.

Kienle, Holger M., and Hausi A. Müller. "The Tools Perspective on Software Reverse Engineering: Requirements, Construction, and Evaluation." *Advances in Computers* 79 (2010): 189-290. https://doi.org/10.1016/S0065-2458(10)79005-7.

Kumar, Rajeev. "Technology Transfer Agreements within the European Union: An Analysis of Block Exemption Regulation." *Journal of Intellectual Property Rights* 19, no. 3 (2014): 229-233. https://nopr.niscpr.res.in/bitstream/123456789/28930/1/JIPR%2019%283%29%20229-233.pdf.

LaRoque, Scott J. "Reverse Engineering and Trade Secrets in the Post-Alice World." *Kansas Law Review* 66 (2017): 427-457. https://kuscholarworks.ku.edu/bitstream/handle/1808/25704/10_LaRoque_Final.pdf?sequence=1&isAllowed=y.

Mahfuzzah, Zenni, Saidin Saidin, Budiman Ginting, and Tanya Karissa Devi. "Non-disclosure Agreements (NDA) as a Legal Protection on Trade Secrets in Work Agreements in Indonesia." *KnowledgeE* 8, no. 21 (2024). https://doi.org/10.18502/kss.v8i21.14768.

Mancaleoni, Anna Maria, and Elise Poillot. *National judges and the case law of the Court of Justice of the European Union*: Proceedings of the conference held in Cagliari, 1st June 2018. Università degli Studi Roma Tre, Dipartimento di Giurisprudenza, 2021. https://romatrepress.uniroma3.it/wp-content/uploads/2021/01/nati-mape.pdf.

Mauk, John E. "The Slippery Slope of Secrecy: Why Patent Law Preempts Reverse-Engineering Clauses in Shrink-Wrap Licenses." *William & Mary Law Review* 43, no. 2 (2001): 819. https://scholarship.law.wm.edu/wmlr/vol43/iss2/7.

Mylly, Ulla-Maija. "*Intellectual property protection of computer program interfaces and interoperability.*" Publications of IPR University Center No. 12. Helsinki, Finland: Oy Nord Print Ab, 2013.

Mylly, Ulla-Maija. "*Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information.*" IIC 54, no. 8 (2023): 1013–1043. https://doi.org/10.1007/s40319-023-01328-5.

Nashkova, Sibela. "*Defining Trade Secrets in the United States: Past and Present Challenges – A Way Forward*?." IIC 54, no. 5 (2023): 634–672. https://doi.org/10.1007/s40319-023-01310-1.

Page, Amy C. "Microsoft: A Case Study in International Competitiveness, High Technology, and the Future of Antitrust Law." *Federal Communications Law Journal* 47, no. 1, Article 9 (1994). https://www.repository.law.indiana.edu/fclj/vol47/iss1/9.

Palmer, Amanda K., and Thomas C. Vinje. "The EC directive on the legal protection of computer software: New law governing software development." *Duke Journal of Comparative & International Law* 2 (1992): 65-87. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1307&context=djcil.

Radauer, Alfred, Nial Searle, and Martin A. Bader. "The possibilities and limits of trade secrets to protect data shared between firms in agricultural and food sectors." *World Patent Information* 73 (2023): 102183. https://doi.org/10.1016/j.wpi.2023.102183.

Republic of Uzbekistan. "*Law on Trade Secrets*, No. LRU-374." 2014. https://lex.uz/ru/docs/6642218.

Saha, Chandra Nath, and Sanjib Bhattacharya. "Intellectual property rights: An overview and implications in pharmaceutical industry." *Journal of Advanced Pharmaceutical Technology & Research* 2, no. 2 (2011): 88–93. https://doi.org/10.4103/2231-4040.82952.

Samuelson, Pamela, and Suzanne Scotchmer. "The Law and Economics of Reverse Engineering." *The Yale Law Journal* 111, no. 7 (2002): 1575–1663. https://doi.org/10.2307/797533.

Sandeen, Sharon K. "Kewanee revisited: Returning to first principles of intellectual property law to determine the issue of federal preemption." *Intellectual Property Law Review* 12 (2008): 299. http://scholarship.law.marquette.edu/iplr/vol12/iss2/3.

Schuldt, Lars. "*EU Copyright and Trade Mark Law: a unifying lens for the protection of Fashion Designs? Analysis and research into a better understanding of the concepts of originality and distinctiveness.*" 2023. https://www.diva-portal.org/smash/get/diva2:1776959/FULLTEXT01.pdf.

Sengar, Dipa Singh. "PROTECTION OF TRADE SECRETS AND UNDISCLOSED INFORMATION: LAW AND LITIGATION."

Journal of the Indian Law Institute 53, no. 2 (2011): 254–274. http://www.jstor.org/stable/43953505.

Shemtov, Noam. "*On reverse engineering and decompilation*." Beyond the Code: Protection of Non-Textual Features of Software. Oxford Academic, 2017. https://doi.org/10.1093/oso/9780198716792.003.0003.

Snider, M., S. Teegavarapu, D. S. Hesser, and J. D. Summers. "*Augmenting Tools for Reverse Engineering Methods." Proceedings of the ASME 2006 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, 371-380. Philadelphia, Pennsylvania, USA: ASME, 2006. https://doi.org/10.1115/DETC2006-99676.

Trallero Ocaña, Teresa. "Chapter 6. *The internal and external spheres of secrecy and their limitations.*" In The Notion of Secrecy, 467-560, 2021. DOI: 10.5771/9783748911975-467.

Verma, S. K. "LEGAL PROTECTION OF TRADE SECRETS AND CONFIDENTIAL INFORMATION." *Journal of the Indian Law Institute* 44, no. 3 (2002): 336–353. http://www.jstor.org/stable/43951824.

Weston, Suriyah. "Improving interoperability by encouraging the sharing of interface specifications." *Law, Innovation and Technology* 9, no. 1 (2017): 78-116. https://doi.org/10.1080/17579961.2017.1302695.

World Trade Organization. "*Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS):* Part II — Standards concerning the availability, scope and use of Intellectual Property Rights, Sections 7 and 8." 1994. https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm.

Yeh, Brian T. "*Protection of Trade Secrets: Overview of Current Law and Legislation.*" CRS Report No. R43714. Congressional Research Service, 2016. https://sgp.fas.org/crs/secrecy/R43714.pdf.