BACKDOOR MAN: A RADIOGRAPH OF COMPUTER SOURCE CODE THEFT CASES

Ioana Vasiu* and Lucian Vasiu

Abstract

The misappropriation of trade secrets threat comes from numerous sources, such as current or former employees, competitors, clients, suppliers, and hackers. Given the fundamental role computer programs play in numerous industries, and taken into consideration the high complexity and financial investments involved in the development process, source code presents a particular interest for perpetrators. Successful misappropriation can result in profound consequences for the victims, compelling strong legal protection. Depending on the nature and circumstances of the offense, the theft of source code can be prosecuted as violation of several statutes, such as the Economic Espionage Act; the Fraud by Wire, Radio, or Television; the Computer Fraud and Abuse Act; the National Stolen Property Act; and the Arms Export Control Act.

Corresponding author: Prof. Dr. Ioana Vasiu, Faculty of Law, Babeş-Bolyai University.This article is part of a large-scale research on cybercrimes, including *Break on Through: An Analysis of Computer Damage Cases*, 14 PGH. J. TECH. L. & POL'Y 158 (2014); *Riders on the Storm: An Analysis of Credit Card Fraud Cases*, 20 SUFFOLK J. TRIAL & APP. ADVOC. 185 (2015); and *Light My Fire: A Roentgenogram of Cyberstalking Cases*, 40 AM. J. TRIAL ADVOC. 41 (2016).

 ISSN 1536-7983.

This article presents a radiograph of cases of theft of source code held as a trade secret, brought to courts in violation of the Economic Espionage Act of 1996, Title 18, Section 1832 of the U.S. Code. The comprehensive study of cases brought under Section 1832 revealed numerous attention holding arguments, issues, and viewpoints, concerning the trade secret definition; the ascertainability and the economic value of the information in dispute; the clarity or effectiveness of the security measures employed; the intent to convert and the moment when the defendant acquired the culpable intent; and loss calculation.

The survey of cases shows that the greatest threat in this regard is posed by actual or former employees, however, the risk of source code theft via data breach or leakage must not be underestimated. This fact strongly recommends more effective employee screening, expected behavior rules, and departing procedures.

The "reasonable" security measures requirement can be understood as "not excessive or extreme," "moderate, especially in price," without the need to employ every conceivable type of measures. The instruction, however, would be clearer if it would use the term "adequate," or "sufficient for the purpose," as the measures do depend on the exact circumstances of each case. Additionally, the adoption of legal or industry standards would be helpful in the process of assessing the capability of the security measures employed.

To increase the legal certainty, the description of the proscribed conduct and of the methodology used in the calculation of loss for sentencing and for restitution should be more precise. As source code theft cases may involve foreign perpetrators or conspirators, efforts should be made to adopt global provisions for the termination of unlawful acquisition, use, or disclosure, as well as cooperation in the bringing of perpetrators to justice.

CONTENTS

I. Introduction

Intellectual property (IP) protection encompasses four major types of rights: copyright; trademark; patent; and trade secrets.[1] Trade secrets, "the most ancient type of intellectual property,"[2] even though "far more amorphously defined than other IP pillars,"[3] represent an important asset of organizations.[4] Trade secrets' role for the competitiveness of companies in the last decades is reflected in the notable efforts aiming to strengthen the legal protection afforded[5] and to identify and monitor countries that deny adequate trade secret protection,[6] as well as in the large number of academic publications focused on various trade secret aspects.[7]

---

[1] *See* Mark A. Lemley et al., *Intellectual Property in the New Technological Age: 2016*, CLAUSE 8 PUBLISHING, 6 (2016) (listing various types of intellectual properties, including trade secrets, patents, copyrights, and trademarks); *see* Brian T. Yeh, CONG. RESEARCH SERV., R43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION 4 (2016) (expounding on the subject matters of intellectual property).

[2] *See* Marco Alexandre Saias, *Unlawful Acquisition of Trade Secrets By Cyber Theft: Between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks*, 9 J. INTELL. PROP. L. & PRAC. 721, 722 (2014).

[3] *See* Orly Lobel, *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, 93 TEX. L. REV. 789, 792 (2015) (explaining how the increase in criminalization in trade secret misappropriations functions to further undermine the boundaries between what is considered protected).

[4] *See* U.S. CHAMBER OF COMMERCE, THE CASE FOR ENHANCED PROTECTION OF TRADE SECRETS IN THE TRANS-PACIFIC PARTNERSHIP AGREEMENT 3 (2013) (emphasizing the value of trade secrets to companies' holdings).

[5] *See e.g.,* 18 U.S.C. § 1836 (2016) (enumerating the grounds under which the holder of a trade secret may bring a civil action against one who is misappropriating a trade secret); Council Directive 2016/943, 2016 O.J. (L 157) 1, 1 (EU) (aiming to standardize the national laws in E.U. countries against the unlawful acquisition, disclosure and use of trade secrets).

[6] *See* 19 U.S.C. § 2242 (2017) (identifying countries that deny adequate protections for intellectual property, according to United States standards); MARK F. SCHULTZ & DOUGLAS C. LIPPOLDT, APPROACHES TO PROTECTION OF UNDISCLOSED INFORMATION (TRADE SECRETS)-BACKGROUND PAPER 4 (OECD PUBLISHING, PARIS 2014) (listing various countries who deny adequate IP protections); OFF. U.S. TRADE REP., 2017 SPECIAL 301 REPORT 2 (2017) (contending that China and India's inadequate protections of trade secrets puts the United States at a greater risk).

[7] David Bohrer, *Threatened Misappropriation of Trade Secrets: Making a Federal (DTSA) Case Out of It*, 33 SANTA CLARA HIGH TECH. L.J. 506, 507 (2017) (asserting that a majority IP theft is committed by employees or partners leaving businesses); Audra A. Dial, *Modern Protection of Business Interests through Trade Secret Enforcement*, 10 J. MARSHALL L.J. 19, 20 (2017) (expounding on the

characteristics and greater protections awarded by trade secrets, as compared to other forms of IP); Michelle Evans, *Plausibility Under the Defend Trade Secrets Act*, 16 J. MARSHALL REV. INTELL. PROP. L. 188, 189 (2017) (discussing the Defend Trade Secrets Act's ("DTSA") plausibility requirements); *see* Lisa Andrukonis et al., *Intellectual Property Crimes*, 53 AM. CRIM. L. REV. 1459, 1462 (2016) (asserting the key areas of IP law that are the basis for criminal prosecutions); Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CAL. L. REV. 1, 3 (2017) (acknowledging that most states have adopted versions of the Uniform Trade Secret Act, with different variations); Molly Hubbard Cash, *Keep It Secret, Keep It Safe: Protecting Trade Secrets by Revisiting the Reasonable Efforts Requirement in Federal Law*, 23 J. INTELL. PROP. L. 263, 266 (2016) (arguing for a federal trade secret law which would set forth various requirements that trade secret owners must take to protect electronically stored trade secret information); Jonathan K. Heath, *Keeping Secrets: The Case for a North American Trade Secret Agreement*, 9 J. BUS. ENTREPRENEURSHIP & L. 411, 412-13, 422 (2016) (proposing the enactment of a North American Trade Secret Agreement); Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57 B.C.L. REV. 381, 383 (2016) (discussing the misappropriation of trade secrets within a cybersecurity framework); David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230, 232-33 (2015) (introducing two bills that would create new protections for victims of trade secret cyberespionage); Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 321-22 (2015) (arguing that trade secrets should be primarily regulated by state law); Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties*, 62 AM. BUS. L.J. 1, 8 (2015) (underlining the importance of bilateral international treaties ("BIT") in fighting trade secret theft); Robert G. Bone, Symposium*: Steps Toward Evidence-Based IP: The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1804 (2014) (arguing that protection for trade secrets "could only be desirable if its social benefits exceed its social costs"); Andrew F. Popper, *More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership*, 12 NW. J. TECH. & INTELL. PROP. 253, 254 (2014) (emphasizing the need for global partnership to better combat IP theft); Andrew Riley & Jonathan Stroud, *Trade Secrets at the International Trade Commission: A Survey*, 15 COLUM. SCI. & TECH. L. REV. 41, 45 (2013) (summarizing the importance of 19 U.S.C. § 1337, as it is used to combat "international white-collar [trade secret] theft"); David S. Almeling, *Seven Reasons Why Trade Secrets are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1092-93 (2012) (emphasizing the growing value of trade secrets and the development of state and federal protections against trade secret misappropriation); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 312 (2008) (discussing theories of how trade secrets are treated as IP rights); Eleanore R. Godfrey, *Inevitable Disclosure of Trade Secrets: Employee Mobility v. Employer's Rights*, 3 J. HIGH TECH. L. 161, 162 (2004) (analyzing a broad overview of court's approaches and suggestions for the simplification of inevitable disclosure of trade secrets); Eric Goldman, *Congress is Considering A New Federal Trade Secret Law. Why?*, FORBES (Sept. 16, 2014), *archived at*

Facilitated by globalization, technological developments, and workers mobility, the opportunities for and the impact of trade secrets misappropriation are on the rise.[8] The theft of trade secrets affects virtually every important economic sector,[9] and imposes severe economic and other harm to the owner of the trade secret and to others.[10] Successful or attempted trade secret theft may result in loss of sales, costs for internal investigation, negotiating settlements, prosecution and litigation, and higher disbursement for security measures.[11] In 2012, for instance, in cases investigated by the FBI's Economic Espionage Unit, the victim companies reported losses amounting to $19 billion.[12]

https://perma.cc/QC5H-T46A (comparing the Trade Secrets Protection Act of 2014 and The Defend Trade Secrets Act of 2014 to the Uniform Trade Secret Act).

[8] *See* U.S. DEP'T OF JUST., SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET AND EMBARGO-RELATED CRIMINAL CASES (2016) (listing major export enforcement, economic espionage, theft of trade secrets, and embargo related criminal prosecutions since January 2010); *see also* LORENZO DE MARTINIS, FRANCESCA GAUDINO & THOMAS S. RESPESS II, STUDY ON TRADE SECRETS AND CONFIDENTIAL BUSINESS INFORMATION IN THE INTERNAL MARKET 4 (2013) (discussing the lack of a uniform definition for "trade secrets" among member states of the European Union).

[9] *See* United States v. Hanjuan Jin, 833 F. Supp. 2d 977, 1007 (N.D. Ill. 2012) (applying EEA's definition of "trade secret" to telecommunications technology); United States v. Chung, 659 F.3d 815, 824-25 (9th Cir. 2011) (summarizing the three prong test used to determine whether something is a "trade secret" under the EEA and applying this test to rocket production technology); United States v. Case, No. 3:06-cr-210TSL-LRA, 2007 WL 1746399, at *4 (S.D. Miss. June 15, 2007) (explaining the EEA's broad definition of "trade secret" as applied to military and commercial aviation hydraulic products); United States v. Dongfan Chung, 633 F. Supp. 2d 1134, 1135 (C.D. Cal. 2009) (examining aerospace and military technologies); SCHWARTZ ET AL., 2013 TRADE SECRETS LITIGATION ROUND-UP (2014) (highlighting various criminal trade secret cases brought by the U.S. government against Chinese entities in cellular glass insulation technology and guidance systems for airborne technology).

[10] *See* OFF. U.S. TRADE REP., 2017 SPECIAL 301 REPORT, 18 (asserting that trade secret theft diminishes U.S. competitiveness abroad and threatens U.S. national security); Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, 57 U.S. ATT'Y BULL. 1, 7 (2009) (reporting that there have been over 100 trade secret prosecutions in the U.S.).

[11] *See* DE MARTINIS, GAUDINO & RESPESS, *supra* note 8, at 142-43 (articulating various consequences of misappropriation).

[12] *See Public Hearing on Proposed Amendments to the Federal Sentencing Guidelines: Hearing on Economic Espionage Before the U.S. Sent'g Commission*, 113th Cong. 29 (2013) [hereinafter, *Hearing on Economic Espionage*] (statement of Louis E. Bladel, III, Section Chief, Counterintelligence Division Federal Bureau of Investigation).

Overall, according to estimates, the theft of trade secrets costs up to $300 billion per year,[13] or 1-3 percent of the U.S. gross domestic product (GDP).[14]

There are multiple trade secret attack vectors.[15] Misappropriation of trade secrets can take the form of economic espionage, which benefits a foreign nation or instrumentality, and theft for pecuniary gain,which benefits an individual or an organization.[16] The threat comefrom numerous sources, such as current or former employees,[17]

[13] *See* DEFEND TRADE SECRETS ACT OF 2016, S. REP. NO. 114-220, at 2 (2016) (assessing losses to the American economy caused by trade secret theft are over $300 billion); *see* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 292 (2010) (highlighting that the theft of trade secrets costs U.S. companies as much as $300 billion per year).

[14] *See* CTR. FOR RESPONSIBLE ENTER. & TRADE & PRICEWATERHOUSECOOPERS LLP, ECONOMIC IMPACT OF TRADE SECRET THEFT: A FRAMEWORK FOR COMPANIES TO SAFEGUARD TRADE SECRETS AND MITIGATE POTENTIAL THREATS 3 (2014) (employing multiple studies on illicit economic activity across the US).

[15] *See* Dept. of Comm. and Def., *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, 1 (Feb. 2013*)* (emphasizing foreign competitor's ability to access trade secrets).

[16] *See* DENNIS C. BLAIR & JON M. HUNTSMAN, JR., THE IP COMM'N REPORT: THE REPORT OF THE COMM;N ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY 24 (NAT'L BUREAU OF ASIAN RES. 2013) [hereinafter, The IP Comm'n Report] (distinguishing economic espionage from the theft of trade secrets).

[17] *See e.g.*, Complaint at 1, United States v. Sazonov, 17 MAG 2798 (S.D.N.Y. 2017) (alleging that the defendant, employed by the victim as a software engineer, attempted to steal and convert source code used in trading systems); Complaint at 1, United States v. Zhang, 17 MAG 2467 (S.D.N.Y. 2017) (alleging that the defendant, employed by the victim company, stole and attempted to convert source code used in a trading system held as trade secret); United States v. Nosal, 844 F.3d 1024, 1041 (9th Cir. 2016) (recounting particular charges against the defendant on appeal, the unauthorized downloading and copying of trade secrets); Fitspot Ventures, LLC v. Bier, No. 2:15-cv-06454-ODW(RAO), 2015 U.S. Dist. LEXIS 116579, at *7-8 (C.D. Cal. Sept. 1, 2015) (summarizing the factual background of the case) The defendant, a software engineer, upon the termination of his relationship with the victim company, in breach of the Confidentiality and Intellectual Property Assignment Agreement, "unlawfully usurped exclusive access to the Company's confidential and proprietary information," and obtained a temporary restraining order, prohibiting the disclosure and use of data and source code. *Id.* United States v. Kim, No. 99-CR-481 (N.D. Ill., July 1, 1999) (reporting that the defendant, while employed as software engineer, copied from his employer source code held as trade secret); Press Release, U.S. Dep't of Just., Futures Trader Indicted For Allegedly Stealing Computer-Stored Trade Secrets From His Former Chicago Trading Firm (Dec. 5, 2014), *archived at* https://perma.cc/PT9G-R65N (publicizing that the defendant, a former futures trader, copied trade secrets onto a personal thumb drive); Press Release, U.S. Dep't of Just., Quincy Man Charged

competitors, clients, suppliers,[18] and hackers.[19] Given the complexity of developing computer programs,[20] the massive financial investments involved,[21] as well as the fundamental role programs play in numerous

With Stealing Former Employer's Intellectual Property (May 8, 2014), *archived at* https://perma.cc/LN9D-EH73 (disclosing that a former employee of a software developer, Daedalus, copied the source code onto a personally-owned hard drive, then went to work for a company where the misappropriated source code was very valuable); Press Release, U.S. Dep't of Just., Former CME Group Software Engineer Indicted for Theft of Globex Computer Trade Secrets While Allegedly Planning Business to Improve Electronic Trading Exchange in China (Sept. 28, 2011), *archived at* https://perma.cc/R2W7-CJGD (reporting that the defendant, a senior software engineer, was charged with downloading over 1,000 files containing one company's source code, subsequently transferred, via flash drives, to his personal computer).

[18] *See* DE MARTINIS, GAUDINO & RESPESS, *supra* note 8, at 139 (demonstrating the extent to which various sources posed a risk of unauthorized access, disclosure, or leakage of trade secrets and confidential business information).

[19] *See* Press Release, U.S. Dep't of Just., Swedish National Charged with Hacking and Theft of Trade Secrets Related to Alleged Computer Intrusions at NASA and Cisco (May 5, 2009), *archived at* https://perma.cc/UDN4-ZAMG (recounting the charges against a Swedish national, including hacking into the network of Cisco and misappropriating Cisco Internetworking Operating System source code, held by Cisco as a trade secret).

[20] *See* Rensselaer Polytechnic Institute v. Apple Inc., No. 1:13-CV-0633, U.S. Dist. LEXIS 63413, 3 (N.D.N.Y. May 8, 2014) (discussing the complexity of Siri's source code). A version of the Siri Natural Language Processing source code contained "nearly 10,000 files alone, distributed over more than 13,000 directories, and contained more than two million lines of code." *Id.* Robert Lagerstrom et al., *Exploring the Relationship Between Architecture Coupling and Software Vulnerabilities: A Google Chrome Case* (Harv. Bus. Sch., Working Paper No. 17-078, 2017) (illustrating the complexities of software component metrics). The complexity of computer programs, or software, can be expressed through a number of metrics, such as the number of source lines of code (SLOC), the cyclomatic complexity (the number of alternative execution paths that could be followed by the program when it runs), or code churn (regarding file activity, in terms of number of lines of code being added, changed, or deleted). *Id. See also* Cade Metz, *Google Is 2 Billion Lines of Code—And It's All in One Place*, WIRED (Sept. 16, 2015), *archived at* https://perma.cc/2TQQ-A9C9 (estimating that Google's Internet services code is approximately two billion lines of code).

[21] *See* United States v. Aleynikov, 737 F. Supp. 2d 173, 175 (S.D.N.Y. 2010) (recounting Goldman Sach's $500 million purchase to obtain the source code misappropriated by the defendant); s*ee also* Complaint at 7, United States v. Xu, 15 MAG 4388 (S.D.N.Y. 2015) (explaining that after "two decades' work," the source code represented "a key component of some of the largest scientific supercomputers, as well as commercial applications requiring rapid access to large volumes of data").

industries, computer source code (source code) can be considered "one of the most critical assets that companies possess".[22]

Source code often present a particular interest for perpetrators,[23] successful misappropriation resulting in profound consequences for victims. In *United States v. Sinovel*, for instance, the defendant misappropriated source code from a company called AMSC, then used it in the operation of wind turbines.[24] As a result of the theft, victim's annual revenues fell by 75 percent, its stock price plummeted by 90 percent, and it had to cut its employee workforce by 70 percent.[25]

This article reports and discusses the main cases of theft of source code held as a trade secret brought to courts in violation of the Economic Espionage Act of 1996, Title 18, section 1832 of the U.S. Code. The article is structured into four parts. Part I looks into definitions of source code and outlines forms of theft. Part II contains remarks on trade secret law and an examination of the legal elements of Section 1832. Part III reports and discusses the most relevant arguments, issues, and viewpoints found in cases brought under the Theft of Trade Secrets Section. Finally, the article outlines the main findings and their normative and managerial implications

[22] *See* Press Release, U.S. Dep't. of Just., Computer Engineer Arrested For Theft Of Proprietary Trading Code From His Employer (Apr. 7, 2017), *archived at* https://perma.cc/E2XP-EMWS (quoting FBI Assistant Director-in-Charge William F. Sweeney Jr.).

[23] *See* United States v. Pu, 814 F.3d 818, 822 (7th Cir. 2016) (comparing the traditional trade secrets data theft case to the circumstances that lead to the defendant's arrest); United States v. Agrawal, 726 F.3d 235, 237 (2d Cir. 2013) (elaborating on the confidential computer source code used to replicate his former employer's trading system); *Aleynikov*, 737 F. Supp. 2d at 187 (recognizing the existence of a ready market for such a valuable trade secret at the time of trial).

[24] *See* United States v. Sinovel Wind Grp. Co., Ltd., 794 F.3d 787, 789 (7th Cir. 2015) (summarizing the defendant's alleged illegal activity).

[25] *See Hearing on Economic Espionage, supra* note 12 at 75 (stating the damages resulting from the crime were in the millions of dollars).

II. Computer Source Code

A "computer program" is "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result."[26] There are three categories of languages in which computer programs can be written: high level, assembly, and machine language.[27] Computer programs are usually written in a high-level programming language, development which provides the source code version of the computer program.[28] In order to run a computer program on a computing device, the program must be compiled or translated from the language in which it was written, into a machine-form (object or binary code), understood by the processor.[29]

The term "source code" is a complex one, difficult to define.[30] In a concise definition, source code is described as "one of several ways to obtain structured binary data that when sequenced to a processor in a particular order causes a computer to perform particular functions."[31] Source code includes text written in languages such as 'C,' 'C++,' assembler, VHDL, Verilog, and/or digital signal processor (DSP) programming languages, and files such as "include," "make," link, or other files "used in the generation and/or building of any software that is directly executed on a microprocessor, microcontroller, or DSP; and accompanying documentation."[32] A comprehensive definition of source code can be found in *Palmchip Corporation v. Ralink Technology Corporation*:[33]

---

[26] *See* 17 U.S.C. § 101 (2010) (defining the term "computer program," statutorily, as a "set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result").

[27] *See* Apple Computer Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1243 (3d Cir. 1983) (comparing three different "levels" of computer language).

[28] *See* Nazomi Commc'ns, Inc.v. Nokia Corp., 739 F.3d 1339, 1340 (Fed. Cir. 2014) (delineating how a software program operates via a computing device).

[29] *See id.* (explaining how the computer program must translate the language from source code to machine code to work).

[30] *See* John Shaeffer, *Software as Text*, 33 SANTA CLARA COMPUTER & HIGH TECH. L.J. 324(2017) (addressing various difficulties that result when attempting to define the meaning of "source code").

[31] *See id.* at 324-25 (applying one meaning of the term "source code").

[32] *See* Linex Tech., Inc. v. Hewlett-Packard Co., No. 4: 13-CV-00159-CW, 2013 U.S. Dist. LEXIS 61808 (N.D. Cal. July 3, 2013) (providing a comprehensive definition of the term "source code"); *see* Protective Order, Comarco Wireless Tech., Inc. v. Apple Inc., No. SACV 15-00145-AG at *8 (C.D. Cal. Aug. 10, 2015) (describing the various forms that source code can take in computer programming).

[33] *See* Protective Order, Palmchip Corp. v. Ralink Tech. Corp., No. 13-1567-MRP

> Human-readable programming language text that defines software, firmware, or electronic hardware descriptions and/or instructions. Source Code includes, without limitation, computer code, scripts, assembly, object code, source code listings and descriptions of source code, object code listings and descriptions of object code, formulas, engineering specifications, or schematics that define or otherwise describe in detail the algorithms or structure of software. Source Code further includes, but is not limited to: (1) printed documents that contain or refer to selected Source Code components; (2) electronic communications and descriptive documents, such as emails, design documents and programming examples, which contain or refer to selected Source Code components, the disclosure of which would create a substantial risk of serious harm that could not be avoided by less restrictive means; (3) electronic Source Code documents that reside in a Source Code repository from which software and related data files may be compiled, assembled, linked, executed, debugged and/or tested; and (4) transcripts, reports, video, audio, or other media that include, quote, cite, describe, or otherwise refer to Source Code, Source Code files, and/or the development thereof. Source Code may further include, but are not limited to, documents containing Source Code in "C", "C++", Java, Java scripting languages, assembler languages, command languages and shell languages. Source Code may further include "header files," "make" files, project files, link files, and other human-readable text files used in the generation, compilation, translation, and/or building of executable software, including software intended for execution by an interpreter.

(SPx), 2014 Cal. Super. LEXIS 1132, at *4-5 (C.D. Cal. Sept. 19, 2014) (providing a definition of the phrase "source code").

Computer programs play a fundamental role in advanced fields, such as radio frequency identification;[34] protection against computer contaminants;[35] computer networking;[36] audio teleconferencing;[37] fleet management;[38] video games;[39] or financial services.[40] The "hybrid nature" of computer programs, allows for multiple IP categorization.[41] The principal modes of legal protection for source code are copyright law,[42] patent law,[43] and trade secret law.[44] Given the actual

[34] *See* Globeranger Corp. v. Software AG United States of America, Inc., 836 F.3d 477, 481 (5th Cir. 2016) (defining Radio Frequency Identification ["RFID"] and how computer programs incorporate RFID).
[35] *See* Trustees of Columbia Univ. v. Symantec, 811 F.3d 1359, 1364-65 (Fed. Cir. 2016) (demonstrating how computers can detect malicious and non-malicious files).
[36] *See* Cisco Sys., Inc. v. Arista Networks, Inc., No. 14-cv-05344-BLF, 2016 WL 4440239 at *1 (N.D. Cal. Aug. 23, 2016) (noting Cisco and Arista's use similar computer programming in the development of their computer network products).
[37] *See* ClearOne Commc'ns, Inc. v. Bowers, 643 F.3d 735, 741 (10th Cir. 2011) (explaining how ClearOne's founder utilized computer programming produce source code to enhance production of audio teleconference equipment).
[38] *See* Beacon Wireless Sol., Inc. v. Garmin Int'l, Inc., 894 F. Supp. 2d 727, 728 (W.D. Va. 2012) (examining how the fleet management industry can be affected when vehicle tracking program are integrated into the industry).
[39] *See* Lilith Games (Shanghai) Co. Ltd. v. uCool, Inc., No. 15-CV-01267-SC, 2015 WL 4149066 at 1* (N.D. Cal. Sept. 23, 2015) (providing an example of an instance of alleged copyright infringement and unauthorized use of the source code of one of video game developer via computer programs).
[40] *See* Tangent Data Serv. LLC v. Hauer, No. 651985/2014, 2015 WL 18886896 at *1 (N.Y. Sup. Ct., 2015) (recognizing the use of computer programs to acquire financial services industries' confidential and proprietary information); Sedosoft, Inc. v. Mark Burchett Ltd., 221 F.Supp.3d 195, 197-98 (D. Mass. 2016) (summarizing the factual background of an instance in which a computer program was developed for financial services firm); Quantlab Tech., Ltd. v. Kuharsky, No. 16-20242, 2017 WL 2713034 at *1 (5th Cir. June 22, 2017) (offering an example of a financial research firm that applies computer programs to identify profitable trading opportunities).
[41] *See* Gregory J. Maier, *Software Protection - Integrating Patent, Copyright and Trade Secret Law*, 69 J. PAT. & TRADEMARK OFF. SOC'Y 151 (1987) (recognizing the "hybrid nature" of software that make it difficult to pigeonhole software into one IP classification); *see also* Peter S. Menell, *Analysis of the Scope of Copyright Protection for Application Programs*, 41 STAN. L. REV. 1045, 1046-47 (1988) (commenting on various differences between the patent system and trade secret law in the context of protecting unique intellectual works).
[42] *See* 17 U.S.C. § 102(a) (2015) (identifying the scope of copyright protections based on their subject matter).
[43] *See* 35 U.S.C. § 101 (explaining what constitutes a "patentable invention").
[44] *See* 18 U.S.C. § 1839(3) (defining trade secrets).

or potential value of source code, it is no surprise that there are numerous cases involving disputes over misappropriation or ownership of source code.[45]

[45] *See* GlobeRanger Corp. v. Software AG U.S., Inc., 836 F.3d 477, 481 (5th Cir. 2016) (affirming judgment in trade secret misappropriation trial against a competitor); Oracle Am., Inc. v. Google Inc., 750 F.3d 1339, 1347 (Fed. Cir. 2014) (summarizing Oracle's case against Google for alleged patent infringement involving its Android mobile operating system); StorageCraft Tech. Corp. v. Kirby, 744 F.3d 1183, 1192 (10th Cir. 2014) (upholding award for $2.92 million after a company director stole source code and disclosed it to a rival company); Arkeyo, LLC v. Cummins Allison Corp., No. 16-4720, 2017 U.S. D. WL 2813224, at *1, 6-7 (E.D. Pa. June 28, 2017) (denying a preliminary injunction for misappropriation of software in coin counting machines for failing to reasonably protect its confidentiality); Compulife Software, Inc. v. Newman, No. 9:16-CV-81942, 2017 U.S. D. WL 2537357, at *3 (S.D. Fla. June 12, 2017) (listing plaintiff's claims against defendant, including possible copyright infringement and theft of trade secrets); Berg v. CI Investments, Inc., No. 15 C 11534, 2017 U.S. D. WL 1304082, at *6 (N.D. Ill. Apr. 7, 2017) (disputing ownership of source code based on the "work for hire" doctrine); Senderra RX Partners, LLC v. Spud Software Co., No. 3: 15-CV-1911-M, 2015 U.S. D. WL 4617179, at *8 (N.D. Tex. Aug. 3, 2015) (enjoining Spud Software Co. from disclosing or utilizing confidential information from Senderra, LLC.); Bartech Sys. Int'l, Inc. v. Mobile Simple Sols., Inc., No. 2:15-cv-02422-MMD-NJK, 2016 U.S. D. WL 3002371, at *7-9 (D. Nev. May 24, 2016) (granting preliminary injunction in part, ordering defendant to halt distribution of services which contain misappropriated trade secrets and return all confidential proprietary information); Autodesk, Inc. v. ZWCAD Software Co., No. 5:14-cv-01409-EJD, 2015 U.S. D. WL 2265479, at *1, 6 (N.D. Cal. May 13, 2015) (denying motion to dismiss because Autodesk adequately alleged wrongful acquisition of their trade secrets); Versata Software, Inc. v. Ameriprise Fin., Inc., No. A-14-CA-12-SS, 2014 U.S. D. LEXIS 30934, at *8-9 (W.D. Tex. Mar. 11, 2014) (addressing breach of contract claims for use of licensed software); Title Trading Servs. USA, Inc. v. Kundu, No. 3:14-cv-225-RJC-DCK, 2014 U.S. D. WL 1765128, at *4-5 (W.D.N.C. May 2, 2014) (granting temporary restraining order against Kundu for sharing unauthorized proprietary information of plaintiff's for profit); Point 4 Data Corp. v. Tri-State Surgical Supply & Equipment, Ltd., No. 11-CV-726 (CBA), 2013 U.S. D. WL 4409434 at *1 (E.D.N.Y. Aug. 2, 2013) (denying plaintiff's alleged claims of unlawful hacking and modification of Point 4 Data's software protections in violation of licensing agreements); Integrated Bar Coding Sys., Co. v. Wemert, No. 04-60271, 2007 U.S. D. WL 496464, at *11–12 (E.D. Mich. Feb. 12, 2007) (denying motion to dismiss because material facts regarding the misappropriation of trade secrets were at issue); Cadence Design Sys., Inc. v. Avant! Corp., 57 P.3d 647, 653-54 (2002) (concluding that the continued misappropriation of a trade secret bolsters a plaintiff's initial claim against a defendant); Advanced Tech. Servs. v. KM Docs, LLC, 767 S.E.2d 821, 823 (Ga. Ct. App. 2014) (affirming summary judgment for improper use of source code by former employees in their new business venture).

The theft of source code, depending on the circumstances of each case, can be prosecuted as violation of several statutes, such as 18 U.S.C. § 1343 (Fraud by Wire, Radio, or Television);[46] 18 U.S.C. § 1831 (Economic Espionage);[47] 18 U.S.C. § 1030(a)(2)(C) (Computer Fraud and Abuse Act);[48] 18 U.S.C. § 2314 (National Stolen Property Act);[49] 22 U.S.C. §§ 2778(b)(2), 2778(c) (Arms Export Control Act);[50] and 18 U.S.C. § 1832 (Theft of Trade Secrets).[51]

[46] *See* United States v. Wang, 898 F. Supp. 758, 759 (D. Colo. 1995) (recounting the District Court's ruling that the defendants' unauthorized transmission by wire of copyrighted computer files contained confidential source code and could be prosecuted as wire fraud); *see also* United States v. Yu Qin, 688 F.3d 257, 258-59 (6th Cir. 2012) (affirming the district court's exclusion of evidence regarding the defendants alleged theft of trade secrets and commission of wire fraud).

[47] *See* Superseding Indictment at 1, United States v. Jiaqiang Xu, No. 7:16CR00010, 2016 WL 3381980, (S.D.N.Y. June 14, 2016) (indicting a defendant for counts of economic espionage, who stole source code from his former employer with the intent to benefit the Chinese Government); *see also* Superseding Indictment at *10-11, United States v. Pang et al., N.D. Cal. (2015) (No. CR-15-00106-EJD) (alleging that defendants conspired to steal trade secrets in order to benefit a foreign government, in violation of § 18 U.S.C. 1831(a)(5)).

[48] *See* United States v. Yihao Pu, 15 F. Supp. 3d 846, 852 (N.D. Ill. 2014) (commenting that the Computer Fraud and Abuse Act is violated when one "intentionally access[es] a computer without authorization or exceed[s] authorized access, and thereby obtain[s] information from any protected computer.").

[49] *See* United States v. Hoskins, 73 F. Supp. 3d 154, 165 (D. Conn. 2014) (clarifying that 18 U.S.C. § 2314 "criminalizes interstate transportation of any stole 'goods, wares, merchandize, securities, or money.'").; *see also* United States v. Agrawal, 726 F.3d 235, 252 (2nd Cir. 2013) (asserting that, for a violation of the National Stolen Property Act to occur, physical control must be exerted over the good or item).

[50] *See* Press Release, U.S. Dep't of Just., Chinese National Sentenced for Economic Espionage, (June 4, 2008), *archived at* https://perma.cc/3VMB-B3WW (noting that defendant Meng violated the Arms Export Control Act by "knowingly and willfully exporting" a defense article to a foreign country without the United States' authorization).

[51] *See* H. Marshall Jarrett et al., *Prosecuting Intellectual Property Crimes*, *in* OLE LITIGATION SERIES, at 159 (OFF. OF LEGAL EDUC., 4th Ed. 2013) (explaining that 18 U.S.C. § 1832 punishes commercial theft of trade secrets when there is economic advantage, regardless of benefits to a foreign government).

III. The Federal Theft of Trade Secret Statute

A. Remarks

IP provides a major contribution to the U.S. GDP and plays a major role in the economic growth and technological progress.[52] In figures, IP-intensive industries furnish over $5 trillion in output, and 74 percent of the U.S. exports.[53] The effective protection of intellectual property rights fulfills a major role in the advancement of innovation, facilitates the creation of new jobs, and stimulates higher research and development (R&D) investments.[54]

Trade secret protection broadly encompasses the following categories: (1) technical data; (2) confidential business information; and (3) know-how.[55] Trade secret law is generally regarded as "based on relational obligations (for example, contract, employment status, or fiduciary duty); property rights; fairness and equity; or unfair competition law tort or delict," however, some legal commentators regard it as a "collection of approaches and norms regarding the protection of business information."[56]

---

[52] *See* The IP Comm'n Report, *supra* note 16 at 24 (noting that the United States economy completely relies on Intellectual Property because nearly every industry uses or produces it); *see also* ECON. AND STATISTICS ADMIN. & U.S. PATENT AND TRADEMARK OFFICE, INTELLECTUAL PROPERTY AND U.S. ECONOMY: INDUSTRIES IN FOCUS vi-viii (Dep't of Com., 2012) (providing examples as to how the intellectual property market expands economic advancement in the U.S.).

[53] *See Hearing on Economic Espionage*, *supra* note 12, at 96 (pointing out how the IP industry provides millions of Americans jobs and generates a substantial amount of revenue).

[54] *See Agreement on Trade-Related Aspects of Intellectual Property Rights* (Jan. 23, 2017), WTO (1st Supp.), at Art. 7 (2017) (expressing the benefits of protected intellectual property rights to promote technological innovation, and social and economic welfare); *see also* Cavazos-Cepeda, R. et al., *Policy Complements to the Strengthening of IPRs in Developing Countries* 5 (Organisation for Economic Co-operation and Development ("OECD"), Working Paper No. 104 2010 (highlighting the "generally positive relationship of IPR reform to trade, foreign direct investment, technology transfer and innovation.").

[55] *See* DOUGLAS C. LIPPOLDT & MARK F. SCHULTZ, UNCOVERING TRADE SECRETS - AN EMPIRICAL ASSESSMENT OF ECONOMIC IMPLICATIONS OF PROTECTION FOR UNDISCLOSED DATA 6 (OECD PUBLISHING, PARIS, 2014), (noting that trade secret protection varies by country but that all customarily focus on "(1) technical information; (2) confidential business information; and (3) know-how").

[56] *See* SCHULTZ & LIPPOLDT, *supra* note 6, at 10 (recognizing the debate in the legal community as to whether trade secret law is based on "relational obligations; property rights; fairness and equity; or unfair competition law tort or delict").

Trade secrets law "serves as a partial substitute for excessive investments in physical security" and "facilitates disclosure in contract negotiations over the use or sale of know-how that otherwise would not occur in the absence of such protection."[57] Another major aim of trade secret law consists in maintaining "standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law."[58] Synthetically, trade secret law can be regarded as a form of "*private* intellectual property law under which creators establish contractual limitations or build legal 'fences' that afford protection from misappropriation."[59]

The legal protection of trade secrets is different from that afforded to patents.[60] Patent owner obtains, for a limited time, "superpowers"[61] over the patented technology, and unauthorized use of that technology by whatever means infringes the patent.[62] Trade secrets, on the other hand, are protected without formal registration, however, standards do exist: information must be secret, must have commercial value because it is a secret, and must have been subject to reasonable steps by the rightful holder of the information to keep it secret (for instance, through confidentiality agreements).[63]

Trade secret protection could be used in combination with other forms of IP protection.[64] The protection afforded to trade secrets is not

---

[57] *See* DE MARTINIS, GAUDINO & RESPESS, *supra* note 8, at 2.
[58] *See* Kewanee Oil Co. v. Bicron Corp. et al., 416 U.S. 470, 476 (1974) (addressing the underlying goals of trade secret law).
[59] *See* Lemley et al., *supra* note 1*,* at I-33 (discussing the origins and purpose of trade secret law and the growing interest in the protection of trade secrets).
[60] *See* Orly Lobel, *Filing for a Patent Versus Keeping Your Invention a Trade Secret*, HARV. BUS. REV. (Nov. 21, 2013), *archived at* https://perma.cc/RHW3-2K9P (comparing the various protections associated with patents and trade secrets).
[61] *See* Kimble v. Marvel Entm't, LLC, 135 S. Ct. 2401, 2406 (2015) (explaining that patents grant the exclusive rights to the patent holder). "[A] patent typically expires 20 years from the day the application for it was filed." *Id.* at 2407.
[62] *See* Katherine Linton, *The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research*, J. OF INT'L COM. & ECON. 1, 4 (2016) (explaining that the first inventor to file a successful application has exclusive patent protections against all others).
[63] *See Agreement on Trade-Related Aspects of Intellectual Property Rights, supra* note 54*,* at Art. 39 (stipulating elements for information to be considered a trade secret under the TRIPS Agreement).
[64] *See Intellectual Property Protection*, UPCOUNSEL (Oct. 5, 2017), *archived at* https://perma.cc/F7EV-N9V5 (comparing intellectual property protections for trade secrets, copyrights, patents, and trademarks).

time-limited, and may be available for inventions that would not qualify for patent protection.[65] For exemplification, a trade secret "may consist of a compilation of data, public sources or a combination of proprietary and public sources."[66] Nevertheless, in certain respects, the protection afforded by trade secret law is significantly weaker than the one under patent law.[67] For instance, trade secrets are not protected "against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering, that is by starting with the known product and working backward to divine the process which aided in its development or manufacture."[68] This means that trade secret owner is protected only in the following situations: "(1) where the secrets were obtained by theft or other improper means, or where they were used; or (2) disclosed in violation of a confidential relationship agreement."[69] The execution of computer programs, however, cannot be considered "use" of the underlying source code, and the program user does not "acquire the requisite knowledge of any trade secrets embodied in that code."[70] On the other hand, if the defendants prove that they developed independently a technique that is similar or resembles the trade secret in dispute, the defendants cannot be held to "use" the trade secret.[71]

---

[65] *See Trade Secret Policy*, USPTO (Oct. 5, 2017), *archived at* https://perma.cc/M4DA-Y2BF (describing how trade secret protection is complimentary to patent protections).

[66] United States v. Nosal, 844 F.3d 1024, 1042 (9th Cir. 2016).

[67] *See* Kewanee Oil Co. v. Bicron Corp. et al., 416 U.S. 470, 476 (1974) (opining that federal patent law and state trade secret law offer different degrees of protection); *see also* Cadence Design Sys. v. Avant Corp., 57 P.3d 647, 650-51 (2002) (comparing the differences in protecting trade secrets versus patents).

[68] *See Kewanee*, 416 U.S. at 476 (explaining that trade secrets are not inviolable).

[69] *See* Lemley, et al., *supra* note 1, at I-33. (enumerating the scenarios under which a trade secret owner is protected from misappropriation) "However, trade secret laws do not protect against independent discovery or invention." *Id.*

[70] *See* Silvaco Data Sys. v. Intel Corp., 184 Cal. App. 4th 210, 216 (App. Ct. 2010) (clarifying that Intel never possessed nor had access to the source code, but only had executable, machine-readable code).

[71] *See* Moore v. Kulicke & Soffa Indus., Inc., 318 F.3d 561, 567 (3rd Cir. 2003) (juxtaposing the use and misappropriation of a trade secret as compared to independently developing a method that merely resembles another's preexisting trade secret).

Trade secret law gives rise to several remedies.[72] According to the specific circumstances, injured owners can obtain criminal penalties, an injunction, damages commensurable with the greater of the owner's loss or the defendant's gain, or a limited injunction.[73]

B. Trade Secrets

Trade secrets are a matter of state law, and consequently the definitions and the protections afforded are, to a certain extent, different.[74] An early definition of "trade secret" can be found in the Restatement (First) of Torts: "may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[75]

The definition of "trade secret" in Title 18, United States Code, Section 1839(3) is:

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
> (A) the owner thereof has taken reasonable measures to keep such information secret; and

[72] *See The Surprising Virtues of Treating Trade Secrets as IP Rights*, *supra* note 7, at 319 (discussing scope of trade secret law with respect to criminal penalties and damages).

[73] *See The Surprising Virtues of Treating Trade Secrets as IP Rights*, *supra* note 7, at 319 (describing how different remedies are based on the type of lawsuit brought).

[74] *See* Cal. Table Grape Comm'n v. RB Sandrini, Inc., No. 1:06-cv-00842-OWW-TAG, 2007 U.S. Dist. LEXIS 48362, at *75-76 (E.D. Cal. June 27, 2007) (noting that state trade secret law is not preempted by federal law, because state law protects different interests).

[75] *See* RESTATEMENT OF TORTS § 757(B) (AM. LAW INST. 1939) (defining "trade secret" as "any formula, pattern, device or compilation of information which is used in one's business, and which gives him any opportunity to obtain an advantage over competitors who do not know or use it.").

> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.[76]

State trade secret laws, the main source of protection against misappropriation for trade secret owners, are similar to the model proposed by the Uniform Trade Secrets Act (UTSA).[77] According to the UTSA, trade secret protection "promotes the sharing of knowledge, and the efficient operation of industry," by "permit[ting] the individual inventor to reap the rewards of his labor by contracting with a company large enough to develop and exploit it."[78] Under the 77UTSA, misappropriation covers (1) acquisition of a trade secret through improper means,[79] and (2) disclosure or use of a trade secret of another without express or implied consent of the secret owner.[80]

Two federal criminal statutes protect against trade secret theft: the National Stolen Property Act (NSPA),[81] criminalizing the transfer of stolen goods (transporting, transferring, or transmitting of any "goods, wares, merchandise, securities or money" with the knowledge that the same has been stolen), and the Economic Espionage Act (EEA),[82] which addresses misappropriation of trade secrets for the benefit of a foreign entity and for monetary rewards or benefits, by making illegal

[76] *See* 18 U.S.C.A. § 1839(3)(A)(B) (2016) (codifying an expansion of the definition of "trade secret").
[77] *See* Uniform Trade Secrets Act With 1985 Amend., 18 U.S.C.S. § 1905 (2016) (approving and recommending for enactment in all the states).
[78] *See* Kewanee Oil Co. v. Bicron Corp. et al., 416 U.S. 470, 493 (1974) (showing Congress's wisdom in allowing the States to enforce trade secret protection).
[79] *See The Surprising Virtues of Treating Trade Secrets as IP Rights*, *supra* note 7, at 321 (recognizing the generally held consensus that "improper means" encompasses more than acts that are already illegal regarding trade secret law).
[80] *See The Surprising Virtues of Treating Trade Secrets as IP Rights*, *supra* note 7, at 318 (highlighting that trade secret rules in case law generally derive from contract law).
[81] 18 U.S.C. § 2314 (2012).
[82] 18 U.S.C. §§ 1831–1832 (1996).

the theft of trade secrets "produced for or placed in interstate commerce",[83] with the knowledge that the offense will injure the owner of the trade secret.[84]

C. Theft of Trade Secrets Under 18 U.S.C. § 1832

Section § 1832(a) provides:

> Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.[85]

In response to the issue raised in *United States v. Aleynikov,*[86]

---

[83] *See* Adam Cohen, *Securing Trade Secrets in the Information Age: Upgrading the Economic Espionage Act After United States v. Aleynikov*, 30 YALE J. ON REG. 189, 214 (2013) (arguing that Congress did not intend to exert its full constitutional authority when drafting the EEA).

[84] *See* 18 U.S.C. § 1832 (codifying the theft of trade secrets); R. Mark Halligan, *Revisited 2015: Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 14 J. MARSHALL REV. INTELL. PROP. L. 477, 487 (2015) (describing how owners derive economic value from trade secrets).

[85] 18 U.S.C. § 1832(a).

[86] United States v. Aleynikov, 676 F.3d 71, 72, 82 (2d Cir. 2012) (overturning the NSPA and the EEA convictions, arguing that the defendant "stole purely intangible property embodied in a purely intangible format", and that Goldman's HFT system "was neither 'produced for' nor 'placed in' interstate or foreign commerce").

Congress passed an EEA amendment, the Theft of Trade Secrets Clarification Act (TTSCA).[87] A significant progress in the legal protection afforded to trade secrets is the Defend Trade Secrets Act (DTSA), formally enacted on May 11, 2016.[88] The DTSA creates a federal, private, civil cause of action for trade-secret misappropriation in which "[a]n owner of a trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[89] The owner of a trade secret can bring a private cause of action in federal court for trade secret misappropriation.[90] In cases in which the defendants are citizens or permanent residents of the United States, or organizations existing under the U.S. laws, the DTSA provisions also apply to conduct outside the U.S.[91]

Forfeiture, destruction, and restitution are subject to Section 2323 and to any other similar legal remedies.[92] Individual offenders may be imprisoned for up to 10 years[93] and incur fines according to 18 U.S.C. § 1832, while organizations can be fine up to $5,000,000.[94] The defendants who attempt to steal trade secrets, or who conspire to steal a trade secret, provided that one or more conspirators performed at least one overt act towards carrying out the conspiracy, face the same sanctions as those who perpetrate the substantive offense.[95]

---

[87] *See* Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012) (codified as amended at 18 U.S.C. § 1831 (2012)) (amended by "striking 'or included in a product that is produced for or placed in' and inserting 'a product or service used in or intended for use in.").

[88] *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2, 130 Stat. 376 (2016) (codified as amended at 18 U.S.C. §§ 1831-1832) (providing "Federal jurisdiction for the theft of trade secrets and for other purposes").

[89] *See* 18 U.S.C. § 1836(b)(1) (2016).

[90] *See id.* (granting the power to bring civil actions for misappropriated trade secrets).

[91] *See* T&S Brass & Bronze Works, Inc. v. Slanina, No. 6:16-03687-MGL, 2017 U.S. Dist. LEXIS 68155, at *38 (D.S.C. May 4, 2017) (finding that because defendants were U.S. citizens or permanent residents, DTSA applies both within and outside the United States).

[92] *See* 18 U.S.C. § 2323 (2008) (delineating various statutorily codified consequences for the wrongful conversion of property); *cf.* 18 U.S.C. § 1834 (2008) (clarifying that the theft of trade secrets falls under 18 U.S.C. § 2323).

[93] *See* 18 U.S.C. § 1832(a) (2016) (limiting the imprisonment of an individual to 10 years for theft of a trade secret).

[94] *See* 18 U.S.C. § 1832(b) (2016) (capping fines for trade secret theft by an organization at $5,000,000).

[95] *See* 18 U.S.C. § 1832(a)(4)-(a)(5) (2016) (listing the possible actions which would result in legal penalties for theft of a trade secret).

D. Legal Elements

According to the U.S. Attorneys' Manual, prosecution under the 18 U.S.C. § 1832 requires the satisfaction of the following six elements: defendant stole, or without owner's authorization, obtained, destroyed, or conveyed information;[96] defendant knew that the information was proprietary; information was a trade secret; defendant had the intent to economically benefit a third party; defendant had the intent to injure the secret owner; and the interstate or foreign commerce nexus.[97]

To establish misappropriation of a trade secret, the plaintiff must prove that it possessed a trade secret and that the defendants are "using that trade secret in breach of an agreement, confidence, or duty, or as a result of discovery by improper means."[98] To prove that something is a trade secret, the prosecution must demonstrate the following: the information was not generally known or readily ascertainable by the public, the secret derived independent economic value from being secret, and that reasonable security measures were in place to protect the secret.[99]

Trade secrets can exist "in a combination of characteristics and components, each of which, by itself, is generally known, or, in other words, is in the public domain, but the unified process, design and operation of which, in unique combination is not generally known and differs significantly from other processes, designs or operations that are generally known."[100] As observed in *United States v. Chung*, while

---

[96] *See* U.S. DEP'T OF JUSTICE, *U.S. Attorney's Manual, Crim. Resource Manual,* §9-59.100 Economic Espionage Act of 1996 (§ 1832) - Prosecutive Policy (2004) (outlining the elements that must be established for the U.S. government to prove a violation of § 1832).

[97] *See id.* (highlighting what the government must establish to prove a violation of 18 U.S.C. § 1832); *see also* United States v. Agrawal, 726 F.3d 235, 251 (2d Cir. 2013) (holding that the government need only prove that at least part of the computer code was involved in interstate or foreign commerce).

[98] *See* 18 U.S.C. § 1839(3)(A)(B) (defining "trade secret"); Integrated Cash Mgmt. Servs, v. Digital Transactions, Inc., 920 F.2d 171, 173 (2d Cir. 1990) (delineating a plaintiff's evidentiary battle where she claims misappropriation of a trade secrets).

[99] *See* 18 U.S.C. § 1839(3) (tailoring the definition of "trade secret"); *See also* United States v. Chung, 659 F.3d 815, 824 -25 (9th Cir. 2011) (discussing the elements the government must show to prove the existence of a trade secrets under the EEA).

[100] *See* ClearOne Commc'ns, Inc. v. Bowers, 643 F.3d 735, 767 (10th Cir. 2011)

the Comment to Section 1 of the UTSA explains that "information is readily ascertainable if it is available in trade journals, reference books, or published materials," the EEA text is slightly different.[101] The explanation that can be given is that Congress "may have intended a more narrow interpretation of 'secret,' that is, the information is secret only if it is not known to or reasonably ascertainable either by the general public or within the industry in which the information has value."[102] In *United States v. Hsu*, for instance, the court understood "the public" as meaning potentially "the economically relevant public," not the "general public."[103] In *United States v. Lange*, on the other hand, the statutory reference in § 1839(3) to "the public" was construed as "the general public — the man in the street."[104]

Even though Section 1832 does not require the prosecution to prove a certain level of value, it must be proven that the trade secret is valuable either to the victim company or to its competitors.[105] The "independent economic value" of the trade secret can be "potential," or "actual."[106] Courts usually "consider the degree to which the secret information confers a competitive advantage on its owner," using a fact-intensive analysis, which, naturally, varies from case to case.[107] The "independent economic value" element can be demonstrated even in cases where the victim company does not have direct competitors

(providing instruction on determining whether a trade secret exists).

[101] *See Chung*, 659 F.3d at 825 (describing how the EEA text is different from how it appears in the UTSA).

[102] *See* CHARLES DOYLE, STEALING TRADE SECRETS AND ECONOMIC ESPIONAGE: AN OVERVIEW OF THE ECONOMIC ESPIONAGE ACT 4 (CONG. RES. SERV., 2016) (explaining Congress's recent trade secret analyses).

[103] *See* United States v. Hsu, 155 F.3d 189, 196-97 (3d Cir. 1998) (clarifying Congress's intent in the EEA to limit the scope of a trade secret).

[104] *See* United States v. Lange, 312 F.3d 263, 266 (7th Cir. 2002) (acknowledging the differences in the function of the word 'public' in the EEA).

[105] *See ClearOne Commc'ns, Inc.*, 643 F.3d at 767 (enumerating the factors used to determine an actual or potential competitive advantage which make a trade secret valuable).

[106] *See* 18 U.S.C. § 1839(3)(B) (1996) (classifying independent economic values as actual or potential).

[107] *See* United States v. Chung, 659 F.3d 815, 826 (9th Cir. 2011) (stating "the degree to which the secret information can create a competitive advantage on its owner[s]" varies "from case-to-case").

for the respective trade secret, provided that the disclosure would confer an advantages to competitors.[108]

There is no "absolute secrecy" requirement for information to be considered a trade secret.[109] It is not required that "no one else in the world possess the information;" instead, it must be determined, taking into account the specific circumstances surrounding the case, if reasonable measures were in place to keep the information secret.[110] Nevertheless, there is no universally accepted definition for what constitutes "reasonable security measures."[111]

In general, security measures include physical, technical, administrative, and contractual components.[112] However, the trade secret owner is not required to take best or all conceivable measures, in order to protect the property from misappropriation.[113] The court in *Rockwell Graphic Sys., Inc. v. DEV*, for instance, underlined that "if trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention."[114] For another illustration, the court in *United States v. Chung*, considered that security measures "such as locked rooms, security guards, and document destruction methods, in addition to confidentiality procedures, such as

[108] *See id.* at 827 (finding that despite having no direct competitors in a project, Boeing derived economic value from keeping documents secret because it would provide competitors with insight into Boeing's efficiency).
[109] *See ClearOne Commc'ns, Inc.*, 643 F.3d at 767 (instructing a jury that total secrecy is not a requirement to determine whether a trade secret exists).
[110] *See id.* (determining trade secrets must have been kept secret, and could not have been made known to the public at large).
[111] *See* United States v. Du, 570 Fed. Appx. 490, 500 (6th Cir. June 26, 2014) (explaining that although there is no one definition of "reasonable measures," and providing examples of certain steps that can be taken to protect sensitive information).
[112] *See id.* at 500-01 (acknowledging GM's policies and practices for keeping trade secrets confidential).
[113] *See* H.R. REP. NO. 104-788, at 7 (1996) (clarifying that the owner must take a "reasonable" measure to safeguard the trade secret).
[114] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991) (proposing that if owners of trade secrets are forced to spend a majority of their time developing more effective trade secret protections, the development of invention will be stifled).

confidentiality agreements and document labeling, are often considered reasonable measures."[115]

The intent to economically benefit a third party element "ensures that the mere possession of trade secrets is not unlawful."[116] The recipient of the intended benefit can be "the defendant, a competitor of the victim, or some other person or entity."[117] There is no requirement for the benefit to be evident is terms of monetary amount.[118]

In *United States v. Hanjuan Jin*, for instance, the court accepted that "the EEA allows employees to economically benefit from the general skills and knowledge that they acquired while working for a former employer."[119] However, the court emphasized that the defendant took "very specific technical data," not general information or skills developed at the place of employment.[120] Consequently, the court reasoned that, "while there was no evidence regarding what the actual economic benefit to Jin would be in terms of a dollar amount, it is clear that she planned to use the documents to her economic benefit by using them to prepare for her next job" and that the "planned use of these documents would also indirectly benefit new employer."[121]

The "intent to injure" element concerns the defendant's state of mind, the prosecution does not have to prove that the trade secret owner lost money as a result of the pilferage.[122] In *United States v. Aleynikov*,[123] for example, the intent to injure the owner of the trade

[115] *See* United States v. Chung, 659 F.3d 815, 825 (9th Cir. 2011) (recognizing security measures that the court deems reasonable).
[116] *See* U.S. v. Hanjuan Jin, 833 F.Supp.2d 977, 1016 (N.D. Ill.2012) (stressing that the Government must show that the defendant had intention to convert trade secrets for economic benefit).
[117] *See* Jarrett et al., *supra* note 51, at 185 (noting that the person receiving the benefit of the stolen trade secrets does not have to be the defendant).
[118] *See Hanjuan Jin*, 833 F.Supp.2d at 1017 (opining that the intended benefit need not be presently quantifiable but can be beneficial in the future).
[119] *See id.* at 1010 (distinguishing what knowledge can and cannot be used by employees for economic benefit, regarding trade secrets, after leaving a company).
[120] *See id.* at 1010-11 (explaining that the defendant was accused of taking confidential information and had specific knowledge of the confidential documents).
[121] *See id.* at 1017 (noting that an economic benefit need be quantified in a dollar amount).
[122] United States v. Hanjuan Jin, 733 F.3d 718, 721 (7th Cir. 2013) (stating that "'independent economic value' attributable to the information's remaining secret need only be 'potential', as distinct from 'actual'" in the lower *Hanjuan Jin* decision).
[123] *See* United States v. Aleynikov, 785 F. Supp.2d 46, 51 (S.D.N.Y. 2011) (explaining what the defendant was charged with after stealing his employer's computer source code near his termination).

secret was established by evidence that the pilfered source code could be used to compete directly with the rightful owner.[124] A similarly understanding of this element can be found in *United States v. Hanjuan Jin*, where the defendant downloaded numerous Motorola proprietary documents.[125] The court argued that "the use or disclosure of the information could give an unfair advantage to a Motorola competitor, thereby harming Motorola," and, "even if the trade secret information never reached the hands of a competitor, the possibility that it could would cause Motorola to take preventative measures to reduce the damage a potential disclosure might cause."[126]

The essence of misappropriation is that the defendant acted "without authorization from the trade secret's owner."[127] A person cannot be prosecuted under this Section if "[a] person [took] a trade secret because of ignorance, mistake, or accident," or in situations in which the person "actually believed that the information was not proprietary after [he took] reasonable steps to warrant such belief."[128] However, prosecution can proceed if a person misappropriated only part of a trade secret.[129]

IV. Litigation Aspects

A. Vagueness Challenges

A criminal statute is void for vagueness if "its prohibitions are not clearly defined,"[130] or defined "in such a way that ordinary people can-

[124] *See id.* at 59 (clarifying that the information stolen would more likely than not result in economic disadvantage to Goldman Sachs).
[125] *See* U.S. v. Hanjuan Jin, 833 F.Supp.2d 977, 1016 (2012) (specifying what information was taken by the defendant without authorization of Motorola).
[126] *See id.* at 1018 (reasoning that the defendant violated all elements of the trade secret statute).
[127] *See* Jarrett et al., *supra* note 51, at 176 (defining authorization to mean "'the permission, approval, consent or sanction of the owner' to obtain, destroy, or convey the trade secret.").
[128] *See* Jarrett et al., *supra* note 51, at 182 (quoting 142 CONG. REC. 27,117 (1996)) (highlighting the exceptions as to when a person cannot be prosecuted for stealing trade secrets, under the EEA).
[129] *See* Jarrett et al., *supra* note 51, at 176 (stating that even when part of a secret is used without authorization, it can be considered misappropriated).
[130] *See* Grayned v. City of Rockford, 408 U.S. 104, 108 (1972) (declaring that criminal statutes that are vague and not clearly defined are void for vagueness).

not understand what is prohibited or if it encourages arbitrary or discriminatory enforcement."[131] In *United States v. Genovese*,[132] the defendant found on the Internet portions of Microsoft Corporation's source code for Windows NT 4.0 and Windows 2000. The defendant posted on his website the following offer: "win2000 source code jacked . . . and illmob.org got a copy of it . . . im sure if you look hard you can find it or if you wanna buy it ill give you a password to my ftp."[133] Following a purchase offer, the defendant allowed access to the source code via his FTP server.[134]

The defendant, charged under Section 1832(a)(2) for selling source code belonging to Microsoft, on the motion to dismiss the indictment, argued that the definition of "trade secret" in Section 1839(3) is unconstitutionally vague in his case, as he found the source code after it had been released to the general public by a third-party, he having "every reason to believe the code had become publicly available."[135] The court, however, considered that defendant's argument "elevates the standard for trade secret status to one of absolute secrecy", whereas "a trade secret does not lose its protection under the EEA if it is temporarily, accidentally or illicitly released to the public."[136] The court underlined that defendant's website posting and sale of the source code were clear indications that he was aware that the source code derived independent value because it was not "generally known."[137]

B. Readily Ascertainable Information

In *United States v. Du*, defendant Du, while working for General Motors (GM), downloaded thousands of GM proprietary documents

[131] *See* United States v. Avant, 907 F.2d 623, 625 (6th Cir. 1990) (*citing* Kolender v. Lawson, 461 U.S. 352, 355 (1983)) (explaining that statutes cannot be so vague that an ordinary person cannot understand what is prohibited).

[132] 409 F. Supp.2d 253, 255 (S.D.N.Y. 2005) (setting forth that the defendant had been indicted with the charges of "downloading, copying, selling, and attempting to sell Microsoft source code without authorization").

[133] *See id.* (quoting defendant's online offer of the source code).

[134] *See id.* (explaining an investigator employed by Microsoft offered to buy the source code for twenty dollars).

[135] *See id.* at 257 (highlighting defendant's argument disputing his liability for trade secret misappropriation).

[136] *See id.* (opining that a trade secret need not be one of "absolute secrecy" under every circumstance).

[137] *See id.* (stating that because defendant knew the code was not generally known as indicated by his language).

onto personal devices.[138] The documents included work-unrelated information that contained GM's motor control source codes and schematics for hybrid motor parts, which the defendants used for a business they started together.[139] The defendants were indicted for conspiracy to possess trade secrets without authorization, in violation of 18 U.S.C. § 1832(a)(5), and unauthorized possession of trade secrets, in violation of 18 U.S.C. § 1832(a)(3) ("motor control source code," which controls the functioning of electric motors)[140].

On appeal, the defendants argued that the information in the GM documents was available in textbooks and online; however, even though there were testimonies that, in general, motor control source codes could be found online, the specific information found in the GM documents was not in the public domain.[141] According to the prosecution's expert, there were no instances of publicly available information with the "level of detail included in the documents," "a few engineers could not independently come up with the technology," and that it would be "inconceivable" that an automaker would distribute such valuable information publicly.[142]

C. Economic Value

The means usually used to establish the economic value element include "showing: (a) competitive advantages for the owner in using the trade secret; (b) the costs for an outsider to duplicate the trade secret; (c) lost advantages to the trade secret owner resulting from disclosure 3to competitors; or (d) statements by the defendant about the value of the trade secret."[143]

---

[138] *See* United States v. Du, 570 F. App'x. 490, 495 (6th Cir. 2014) (explaining how a former GM employee misappropriated trade secrets).
[139] *See id.* (detailing how *Du* and *Qin* used the stolen information to create a joint venture to sell competing products, such as hybrid vehicle motor control systems).
[140] *See id.* (listing the three counts that *Du* was indicted on regarding alleged trade secret violations).
[141] *See id.* at 501 (summarizing the defense's position regarding the second element of the definition of "trade secret").
[142] *See id.* (explaining government's argument that the surrounding circumstances would prevent the automaker from publicly distributing these trade secrets).
[143] *See* Krotoski, *supra* note 10, at 11 (elucidating the third part of the definition of trade secret: whether the information has "independent economic value").

In *United States v. Aleynikov*,[144] the defendant was a former computer programmer for Goldman Sachs.[145] Aleynikov stole Goldman's proprietary computer source code towards the end of his employment with the firm, with the intent to use the pilfered code at his new employer.[146] The defendant attempted to demonstrate that the stolen source code did not have independent economic value, therefore he could not have harmed Goldman Sachs or benefited himself by stealing the source code.[147] However, one of the prosecution's experts testified that "the components stolen by Aleynikov would be highly valuable to a competitor as stand-alone items."[148] A former computer programmer in Goldman Sachs' quantitative trading group also testified that the application from which the defendant took the source code had no "dependencies," in other words it would not require another part of the software to function.[149] Consequently, the defendant's motion was considered without merit and denied.[150]

D. Reasonable Security Measures

"Reasonable" means "being in accordance with reason, fairness, duty, or prudence," "supported or justified by fact or circumstance," "not excessive or extreme," "moderate, especially in price."[151] "Security" is a "condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its

[144] 676 F. 3d 71, 72 (2d Cir. 2012) (outlining the government's case in a trade secret dispute).
[145] *See id.* at 73 (describing defendant's employment with Goldman Sachs & Co.).
[146] *See id.* at 74 (explaining the defendant's alleged theft of Goldman Sachs & Co.'s trade secrets occurred just before his "going away" party).
[147] *See* United States v. Aleynikov, 785 F.Supp.2d 46, 76 (2011) (recounting the defendant's argument that he would have needed access to the entire Goldman Sachs trading platform to harm Goldman Sachs and/or benefit himself).
[148] *See id.* at 77 (employing expert testimony to dispute Aleynikov's assertion, claiming that the stolen components would be highly valuable to a competitor as stand-alone items).
[149] *See id.* (explaining "dependencies," as it relates to the Goldman Sachs & Co. software that was stolen by the defendant).
[150] See *id.* at 79 (concluding Aleynikov failed to demonstrate that the government summation deprived him of a fair trial).
[151] *See Reasonable*, MERRIAM-WEBSTER.COM (Oct. 12, 2017), *archived at* https://perma.cc/2WGA-TUGM (defining the legal definition for reasonable); *see also Reasonable*, THEFREEDICTIONARY.COM (Oct. 12, 2017), *archived at* https://perma.cc/HBE9-SGSQ (giving the general public's definition of reasonable).

mission or critical functions despite risks posed by threats to its use of information systems."[152] Security measures must commensurate with the level of sensitivity and the risks identified.[153] Protective security measures "may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach."[154]

"Reasonable measures" consist usually of a "layered or tiered approach."[155] The first layer concerns physical security, such as "isolating the trade secret to a particular area and limiting access on a "need to know" basis; using security cards to monitor and restrict access; or requiring sign-in sheets to record visitors."[156] A second layer regards technical measures, such as authentication, encryption, and firewalls.[157] To negatively affect the readability or usability of the source code, owners can also use obfuscating transformations.[158] Finally, the security protection is complemented with "employment policies and practices including employee non-disclosure agreements, marking trade secret and proprietary information as 'confidential,' training and reminders about the importance of protecting the company trade secrets, employment manuals, and exit interviews upon an employee's departure to ensure proprietary materials have been returned and to underscore confidentiality obligations."[159]

---

[152] *See* NAT'L. INST. OF STANDARDS AND TECH., GLOSSARY OF KEY INFORMATION SECURITY TERMS 167 (Richard Kissel, Rev. 1 2011) (defining security in the context of the National Institute of Standards and Technology).

[153] *See id.* at 156 (explaining residual risk as potential to lose information even after all IT security measures are applied).

[154] *See id.* at 167 (illustrating different protective measures).

[155] *See* Krotoski, *supra* note 10, at 10 (quoting language describing multiple levels of security).

[156] *See* Krotoski, *supra* note 10, at 10 (providing examples of measures which physically secure information).

[157] *See* Krotoski, *supra* note 10, at 10 (describing additional technical protections one may take to secure trade secrets from being stolen).

[158] *See* Krotoski, *supra* note 10, at 10 (suggesting another way in which one could meet the requirement of taking reasonable measures to ensure that the source code is not easily stolen).

[159] *See* Krotoski, *supra* note 10, at 10 (listing employment practices which help increase confidentiality).

There is no need for the owner to employ every category of security measures in order to satisfy this trade secret requirement.[160] In *Integrated Cash Management Services, Inc. v. Digital Transactions*, the defendant, upon ending the employment with the plaintiff, took a copy of source code he had written for ICM.[161] The security measures in the case included locked doors and nondisclosure agreements, which provided that "[w]hen employment is terminated, the [former employee] agrees not to use, copy or disclose any of ICM's secrets, software products, software tools or any type of information and software which belongs to ICM," were considered reasonable by the court.[162]

In *United States v. Biswamohan Pani*, the defendant, while already on the payroll of a competitor of Intel, downloaded "top secret" files, describing processes for Intel's newest microprocessors.[163] The security measures instated by the victim company included confidentiality agreement, requiring all employees to avoid disclosing secrets; restrictive physical access measures; encryption of confidential documents; password-enabled or token-controlled access to sensitive information; and recording of employees' access and downloading of confidential documents.[164]

The clarity or effectiveness of security measures may be challenged by the defendants.[165] In *United States v. Du*,[166] for instance, the

[160] *See* Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, 57 U.S. ATT'Y BULL. 1, 9-10 (2009) (exemplifying a court's intent to not preclude owners from recovering under the trade secrets act by requiring them to exhaust every reasonable step).

[161] *See* Integrated Cash Mgmt. Serv. v. Digital Transactions, Inc., 920 F.2d 171, 172 (2d Cir. 1990) (recounting how defendant stole source code he had authored for ICM, his previous employer).

[162] *See id.* at 174 (finding that ICM had taken reasonable measures to protect its trade secret).

[163] *See* Government's Motion for Summary Disposition Pursuant to Local Rule 27(c) at *3-4, United States v. Biswamohan Pani, 2013 U.S. 1st Cir. Briefs Lexis 362 (2013) (No. 12-2054) (outlining the facts surrounding the defendant's charges during his employment at Intel).

[164] *See* Brief of Defendant-Appellant Biswamohan Pani at 11, United States v. Biswamohan Pani, 2013 U.S. 1st Cir. Briefs Lexis 362 (2013) (No. 12-2054) (addressing the defendant's stance that there was limited damage because the corporation's files were encrypted even after being taken).

[165] *See* 570 F. App'x. 490, 501 (6th Cir. 2014) (summarizing the defendants' argument that GM's security measures were unclear and therefore unreasonable).

[166] *See id.* at 500 (explaining functions of security guards at the locked facility).

facility where the defendant worked, was locked and monitored constantly by security guards.[167] The guards required employees to show a photo identification for those that wanted to enter, and checking all bags and computer devices carried out of the building, patrolling the facility after hours, and escorted visitors within the facility.[168] The victim company also had "formal policies and practices governing confidentiality and information security," including "non-disclosure agreements signed by employees and an information security policy requiring employees to protect the company's proprietary information and limiting their access to this information on a 'need to know basis.'"[169] Security included technical measures designed to prevent access of unauthorized users.[170] The access to certain folders required an additional password and permission from a manager, who "authorized access only if an employee needed the files for work."[171] The defendants, however, argued that GM's policies "suffer[ed] from a lack of clarity and . . . a lack of enforcement," rendering them unreasonable, specifically the defendants mentioned the GM's classification policy.[172] GM's chief information security officer explained, however, that "marking a document increased the security protocols governing that document, making sharing between engineers more cumbersome," consequently such inconsistencies were considered irrelevant.[173]

E. Intent to Convert

Conversion is defined as:

> [t]he wrongful possession or disposition of another's property as if it were one's own; an act or series of acts of willful interference, without lawful justification,

[167] *See id.* (listing the physical security measures taken by facility including the tasks required of security personal for their daily routines).
[168] *See id.* (specifying the security guard's responsibilities in monitoring the locked facility).
[169] *See id.* at 500-01 (expounding further on GM's security practices).
[170] *See Du*, 570 F. App'x at 501 (describing the technical security measures implemented by GM, such as a password-protected firewall on their servers).
[171] *See id.* (detailing the substantial security measures taken to protect access to server).
[172] *See id.* (summarizing the defendant's argument that GM's policies were ambiguous).
[173] *See id.* (asserting that it was possible for a jury to consider these classification policy inconsistencies as irrelevant).

> with any item of property in a manner inconsistent with another's right, whereby that other person is deprived of the use and possession of the property.[174]

As intent may not be proven directly, the courts looks to the circumstances surrounding defendant's actions.[175] If the intent to convert is not proven beyond a reasonable doubt, the defendant will be acquitted.[176]

In *United States v. Du*, co-defendant Qin raised the argument that he did not intend to convert the GM trade secrets because "he could not have known the documents contained secret information."[177] The court, however, considered that "this is undermined by his experience as an engineer."[178] Further, a government witness testified that the defendants' company used trade secrets information in the GM files for a project.[179]

In *United States v. Agrawal*, the defendant, employed by a bank (SocGen), had access to confidential computer code, used in high frequency securities operations.[180] The defendant abused his position of trust by printing source code on paper, then physically transporting the printouts to his home.[181] The defendant, was convicted for violations of the EEA and the NSPA.[182]

---

[174] *See* DOYLE, *supra* note 102, at 3 (defining "conversion").
[175] *See* United States v. Shiah, No. SA CR 06-92, 2008 WL 11230384, at *20 (C.D. Cal. Feb. 19, 2008) (commenting how the court examined the surrounding circumstances, to determine a lack of requisite intent).
[176] *See id.* at *25 (holding the Government did not prove beyond a reasonable doubt that the defendant, at his new workplace, intended "to do more than using general knowledge, skills, and information obtained at Broadcom. . .."); *see also* United States v. Sing, No. CR 14-212 (A)-CAS, 2016 WL 54906, at *15 (C.D. Cal. Jan. 4, 2016) (declaring no evidence was presented to show that the defendant shared trade secrets with any third parties).
[177] *See* United States v. Du, 570 F. App'x. 490, 502 (6th Cir. 2014) (quoting codefendant's argument).
[178] *See id.* at 502 (opining that codefendant's experience as an engineer undermined his defense).
[179] *See id.* at 495 (describing defendant's company had previously used trade secrets in GM files).
[180] *See* United States v. Agrawal, 726 F.3d 235, 237 (2d Cir. 2013) (describing defendant's position of employment at SocGen).
[181] *See id.* (discussing defendant's decision to take home code printouts).
[182] *See id.* (listing charges that the defendant faced and the legal questions which determine the result).

At appeal, the defendant denied that, "at the exact time he transported each stack of copied code from New York to New Jersey, his intent was to steal or convert it," explaining that he "intended to use the code for his employer's benefit, following a request from his supervisor to work from home on a project."[183] The defendant, nevertheless, decided later to convert the source code for his own benefit and for the benefit of a company that engaged to pay the defendant hundreds of thousands of dollars, to reproduce the trading system of the victim company's trading system for their use.[184] However, the district court argued that the prosecution does not have to prove that the defendant had the required "culpable intent at the precise time he printed and removed the HFT code from SocGen's New York offices," and concluded that "the EEA's intent element could be satisfied by proof that the defendant possessed the requisite intent to convert when he "removed the code or at any point thereafter when he was still in unauthorized possession of the computer code."[185] The defendant contended that "the district court erred as a matter of law by effectively instructing the jury that, 'if Agrawal formed an intent to convert [SocGen's HFT] code after he had copied and/or removed it, that intent could somehow relate back to the initial act and render it criminal.'"[186] Even though the unauthorized transfer was concluded on distinct days, defendant's possession was uninterrupted for about ten months, even past his resignation from SocGen.[187] Taking all these into consideration, the appeals court considered that the district court correctly recognized that, "as a matter of law, the government could carry its burden on the element of intent if it proved the requisite mens rea 'when [Agrawal] removed the code, or at any point thereafter when he was still in unauthorized possession of the computer code.'"[188]

[183] *See id.* at 240 (repeating the defendant's assertion that he never intended to steal or convert trade secrets).
[184] *See id.* at 238-39 (recounting that the defendant eventually stole SocGen's trading systems and was in discussions with competitor to replicate SocGen's practices in exchange for hundreds of thousands of dollars).
[185] See *id*. at 240-41 (explaining that the intent element could be satisfied by evidence the defendant possessed "the requisite intent to convert when he took the computer code").
[186] See *Agrawal.*, 726 F.3d at 255 (recounting the potentially erroneous jury instructions).
[187] See *id.* at 256 (observing that the defendant maintained possession of computer code printouts after his resignation).
[188] *See id.* at 256 (noting the district court's correct recognition the intent element was proven).

F. Loss Calculation and Sentencing

The general rule in loss calculation is that the court determines the greater of actual or intended loss.[189] Actual loss is calculated as "the reasonably foreseeable pecuniary harm that resulted from the offense," while "intended loss" is determined as the "pecuniary harm that was intended to result from the offense and includes intended pecuniary harm that would have been impossible or unlikely to occur (e.g., as in a government sting operation, or an insurance fraud in which the claim exceeded the insured value)."[190] Trade secrets thefts cases, nevertheless, do not involve loss of tangible property, sometimes not even actual loss.[191] While the determination of trade secrets value is a difficult task, however, the court must at least provide an estimate and reasons for it.[192] The calculation of loss for sentencing purposes can be different from loss calculation for purposes of restitution.[193]

An illustrative case in this category is *United States v. Pu*.[194] The defendant copied to personal storage devices files that were part of each company's proprietary software that allowed them to execute strategic trades at high speeds.[195] The defendant used the data acquired to conduct computerized stock market trades for himself, losing about $40,000.[196] The district court found that the intended loss amount was $12,294,897, which resulted in a twenty-level sentence increase.[197]

The intended loss is often used to capture the loss the victim would or could have suffered had the offender been able to complete

---

[189] *See* U.S.C.S. § 2B1.1(c)(4)(3)(A) (LexisNexis 2015) (codifying several definitions of "loss").
[190] *See id.* (stating the definitions of actual and intended loss).
[191] *See* William P. Campos, *Loss Amount in Trade Secret Cases*, 64 U.S. ATT'Y BULL. 14, 15 (2016) (recognizing that, oftentimes, trade secret theft cases involve "no loss of tangible property or even actual loss").
[192] *See* United States v. Howley, 707 F.3d 575, 583 (6th Cir. 2013) (claiming the court needs to provide an estimate of loss and reasons why).
[193] *See* United States v. Hunter, 618 F.3d 1062, 1065 (9th Cir. 2010) (outlining the differences between sentencing and restitution guidelines); U.S. Sent'g Comm'n, *Loss Calculations Under § 2B1.1(b)(1)* 1 (June 2015).
[194] *See* United States v. Pu, 814 F.3d 818, 821-23 (7th Cir. 2016) (providing the facts of the case in which Pu illegally copied confidential files containing trade secrets).
[195] *See id.* (describing the defendant's criminal actions).
[196] *See id.* at 821 (detailing defendant's monetary losses amounting to nearly $40,000).
[197] *See id.* at 822-3 (providing reasoning for the defendant's sentence increase).

his interrupted criminal scheme.[198] In *Pu*, for instance, the district court found that the government did not prove that Pu was interrupted before completing a criminal act, and considered that the district court did not explain how Pu intended to cause a $12 million loss through his conduct, whether by considering charged conduct or relevant conduct.[199] The defendant argued that the proper loss calculation for sentencing in his case should have been zero, as he did not intend to financially injure the victims of his misappropriation.[200]

The court, however, pointed out that the essential question in this case is whether the prosecution "proved by a preponderance of the evidence that the cost of development of the trade secrets was the correct loss figure."[201] As the defendant did not have the intent to cause the victims a loss equal to the cost of development, the district court's use of the cost of development to determine the intended loss amount was deemed inappropriate.[202] Consequently, the appeal court remanded the case for resentencing.[203]

VI. Conclusion

Source code plays an essential role for the competitiveness of companies. As the actual or potential consequences of source code theft can be very significant, the protection must be considered of paramount importance. While the risk of source code theft via computer breaches must not be downplayed, the survey of cases brought to federal courts reveals that the greatest threat in this regard is posed by actual or former employees. This fact strongly recommends more effective employee screening, expected behavior rules, and departing procedures.

---

[198] *See id.* at 827 (explaining that intended loss usually encompasses "the loss the victim would or could have suffered "had the offender been able to complete his interrupted criminal scheme").

[199] *See Pu*, 814 F.3d at 827 (observing the district court findings that the government failed to explain how the defendant intended to cause $12 million in loss).

[200] *See id.* at 828 (reasoning the district court findings that the statute of conviction does not explicitly require economic loss to the victim).

[201] *See id.* at 826 (determining the standard used by lower court was incorrect when attributing the economic loss to the defendant).

[202] *See id.* (concluding the record does not show the defendant's intent to cause the victim an economic loss).

[203] *See id.* at 827 (holding the lower court made an error when calculating his sentence as well as the restitution value).

The reliance on the legal protection of source code should be complemented by effective security measures. Such measures should include confidentiality agreements; clear policies regarding the classification, acceptable use, and storage of secret information; explicit restrictions on the use of e-mail and other electronic communication forms and of photographic devices, and mandatory duties upon employment termination; encryption or obfuscation techniques; periodic reviewing of access lists and rights and of data breach response plans; monitoring and logging of network, USB, and printing activity with specialized software; and proper training for the persons in charge of protecting the source code.

Clearer description of the proscribed conduct and of the methodology used in the calculation of loss for sentencing and restitution would increase the legal certainty. Regarding the "security measures" requirement, for increased clarity, the instruction should use the term "adequate," or "sufficient for the purpose," instead of "reasonable," as the measures considered sufficient depend on the exact circumstances of each case. Further, legal or industry standards would be very helpful to address the challenges regarding the reasonable security measures that need to be in place for trade secrets, as well as in assisting organizations in designing adequate protection for confidential information.

Considering that, in certain cases, the prohibited conduct, requires advanced education or training, the sophisticated means enhancement[204] should also be considered in sentencing. Finally, global uniform legal protection of trade secrets should be envisaged. Such protection would comprise effective and efficient provisions for the termination of unlawful acquisitions, uses, or disclosures of a trade secret, cooperation in the bringing of perpetrators to justice, and adequate civil compensation.

[204] *See* U.S. Sent'g Comm'n, *Guidelines Manual §2B1.1(b)(10)(C)(3)(A)(i-ii)* 96 (Nov. 2015) (defining the basic economic offenses dealing with larceny, embezzlement, and other forms of theft).