THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOLUME XXIV STLR.ORG FALL 2022

NOTE

DATA MISAPPROPRIATION: A TRADE SECRET CAUSE OF ACTION FOR DATA SCRAPING AND A NEW PARADIGM FOR DATABASE PROTECTION

Geoffrey Xiao*

Data scraping (also called web scraping, screen scraping, or web crawling) is a technique that uses "bots" to automate the collection of information from publicly available websites. Fundamentally, data scraping is data copying. Intellectual property ("IP") law—namely, copyright—typically handles disputes involving copying. However, copyright law largely fails to protect data and databases (i.e., compilations of data). Instead, plaintiff websites assert contract law, Computer Fraud and Abuse Act ("CFAA"), and state unfair competition law (common law misappropriation, unjust enrichment, conversion, and trespass to chattel) claims against data scrapers.

This Note proceeds as follows. First, this Note examines how scrapers can be liable under trade secret law for scraping data from publicly accessible websites. Initially, trade secret law seems incongruous with data scraping because the core concept of trade secret law—secrecy—is seemingly at odds with public accessibility. If a website is publicly available, how can a scraper be liable for trade secret misappropriation of the website's data? This Note explains how a recent Eleventh Circuit case, Compulife Software Inc. v. Newman, *laid the groundwork for a trade secret cause of action. This Note reconciles* Compulife *with existing trade secret jurisprudence, argues that* Compulife *was rightly*

*Columbia Law School, J.D., 2021. Many thanks to Professor Clarisa Long for her invaluable insights and guidance, the wonderful staff of the Columba Science and Technology Law Review for their thorough edits, and Qifan Huang for many fruitful discussions.

decided as a matter of both law and policy, and provides a roadmap for courts to apply trade secret law to data scraping cases.

Second, this Note explains why courts and litigators should use trade secret law to adjudicate data scraping disputes. Specifically, this Note argues that, compared to the existing alternatives, trade secret law is best suited to handle the various policy issues surrounding data scraping. This Note explains how contract law and the CFAA have filled the database void left by copyright law: contract law and the CFAA have become "quasi-IP" regimes, granting websites property rights in databases otherwise unprotected by copyright law. In response to the emergence of quasi-IP, this Note argues for reconceptualizing the data scraping problem by reframing data scraping as data copying—reframing data scraping with an intellectual property lens. Trade secret law offers a framework for that reconceptualization. In contrast to contract law and the CFAA (an anti-hacking law premised on criminal trespass principles), trade secret law provides courts and litigators with the appropriate IP-based doctrinal levers to analyze data scraping cases.

Finally, this Note analyzes how EU law filled the database gap by creating an IP right, the sui generis *database right. This Note argues that* Compulife*'s trade secret theory emulates many aspects of the EU* sui generis *database right. In this sense,* Compulife*'s trade secret theory can be seen as the United States' attempt to fashion its own* sui generis *database right to fill the database gap left by copyright.*

I. INTRODUCTION

The global economy runs on data.[1] As technological capabilities have increased, society has entered the "Big Data" era.[2] Driving this data revolution are databases, which are "collection[s] of independent works, data or other materials arranged in a systematic or methodical way."[3] ESPN's website on sports statistics, for instance, is a massive database.[4] Similarly, a database undergirds Yahoo! Finance's data on financial markets[5] and Airbnb's catalog of rentals.[6]

This Note analyzes how data "scrapers" use automated means (i.e., "bots") to extract data from publicly available websites like ESPN, Yahoo! Finance, and Airbnb, as well as their underlying databases.[7] Given the value and utility of data, scraping has abounded, and a cottage industry of scraping services has emerged.[8] According to one estimate, data scraping accounts for 37% of all web traffic.[9] Websites, however, have expended immense amounts of effort to create databases—scrapers copying from databases free ride on a website's labor, threatening the website's economic livelihood.[10]

---

[1] Louis Columbus, *10 Charts That Will Change Your Perspective Of Big Data's Growth*, FORBES (May 23, 2018, 7:02 AM), https://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/?sh=53c9d9c02926.

[2] *Big Data*, SAS, https://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited Jan. 30, 2021).

[3] Council Directive 96/9/EC, art. 1(2), 1996 O.J. (L 77) 20 (EC), [hereinafter Database Directive]. The Database Directive created the EU *sui generis* database right, which is discussed *infra* Section VI.

[4] ESPN, https://www.espn.com/ (last visited Jan. 30, 2021).

[5] YAHOO! FINANCE, https://finance.yahoo.com/ (last visited Jan. 30, 2021).

[6] AIRBNB, https://www.airbnb.com/ (last visited Jan. 30, 2021).

[7] *What is data scraping?*, CLOUDFLARE, https://www.cloudflare.com/learning/bots/what-is-data-scraping/ (last visited Jan. 20, 2021).

[8] *See, e.g.*, DATAHUT, https://datahut.co/ (last visited Jan. 30, 2021).

[9] Edward Roberts, *Bad Bot Report 2020: Bad Bots Strike Back*, IMPERVA (Apr. 21, 2020), https://www.imperva.com/blog/bad-bot-report-2020-bad-bots-strike-back/.

[10] *See* Compulife Software Inc. v. Newman, 959 F.3d 1288 (11th Cir. 2020); Alison Frankel, *Instacart goes after Uber in data-scraping war with Cornershop*, REUTERS (Jan. 14, 2021, 4:25 PM), https://www.reuters.com/article/legal-us-otc-instacart-idUSKBN29J2SY.

But while websites have legitimate claims to their databases, scrapers and society have equally strong interests in competition and the dissemination of information. Scraping can be immensely beneficial to society as a whole: for example, researchers scraped data from Airbnb to study housing discrimination.[11] First Amendment values also underlie scraping, as courts have developed a "right to record" under the First Amendment, protecting information gathering activities such as filming police activity.[12] This "right to record" is directly applicable to scraping, especially scraping performed for research and journalistic purposes.[13]

Finally, the dominance of Big Tech and the ability of "data-opolies" to control data and kill competition also caution against giving websites with dominant market positions too much control over their databases.[14] In other words, access to data is tantamount to access to the market, and limiting scraping stymies competition. Ultimately, data scraping presents a complex, high-stakes problem. How we solve the problem—the allocation of data rights among the various interested parties—implicates the future of the Internet and Big Data.

Plaintiff websites who created databases have typically brought Computer Fraud and Abuse Act ("CFAA"),[15] copyright,[16] breach of contract,[17] and various unfair competition (common law misappropriation, unjust enrichment, conversion, and trespass to chattel)[18] claims against scrapers. Until the recent Eleventh Circuit case *Compulife Software Inc. v. Newman*, trade secret law was not considered as an avenue for data scraping litigation because the consensus was that trade secret law

---

[11] *See* Benjamin Edelman & Michael Luca, *Digital Discrimination: The Case of Airbnb.com*, HARVARD BUSINESS SCHOOL (Jan. 10, 2014), https://www.hbs.edu/faculty/Pages/item.aspx?num=46073.

[12] *See* S.H.A.R.K. v. Metro Parks Serving Summit Cty., 499 F.3d 553, 560 (6th Cir. 2007); *see also* Jacquellena Carrero, Note, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision*, 120 COLUM. L. REV. 131, 151–154 (2020); Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014) (arguing data scraping is speech); Geoffrey Xiao, Note, *Bad Bots: Regulating the Scraping of Public Personal Information*, 34 HARV. J.L. & TECH. 701, 727–31 (2021).

[13] Carrero, *supra* note 12, at 154–158.

[14] *See generally* Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 GEO. L. TECH. REV. 275 (2018) (arguing that we should be concerned about data-opolies).

[15] *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1201 (9th Cir. 2022); *see also* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 390 (2018) (collecting all decided CFAA cases).

[16] *See, e.g.*, Ticketmaster Corp. v. Tickets.com, Inc., No. 99CV7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000), *aff'd*, 2 F. App'x 741 (9th Cir. 2001).

[17] *See, e.g.*, Int'l Council of Shopping Centers, Inc. v. Info Quarter, LLC, No. 17-CV-5526 (AJN), 2019 WL 2004029, at *4 (S.D.N.Y. May 7, 2019); Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 426 (2d Cir. 2004).

[18] *See, e.g.*, Allure Jewelers, Inc. v. Ulu, No. 1:12CV91, 2012 WL 4322519, at *2–4 (S.D. Ohio Sept. 20, 2012) (common law misappropriation); Snap-on Bus. Sols. Inc. v. O'Neil & Assocs., Inc., 708 F. Supp. 2d 669, 680–82 (N.D. Ohio 2010) (unjust enrichment); QVC, Inc. v. Resultly, LLC, 159 F. Supp. 3d 576, 599 (E.D. Pa. 2016) (conversion); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1065–71 (N.D. Cal. 2000) (trespass to chattel).

did not protect publicly available (and hence scrape-able) databases.[19] After all, how can publicly available information be a trade secret? This Note analyzes how the *Compulife* decision created a trade secret cause of action for data scraping and argues that courts and litigators should embrace *Compulife*'s trade secret law theory to analyze data scraping cases.

Section II provides a brief overview of the alternative causes of action to trade secret law and their shortcomings. Next, Section III provides factual background on the *Compulife* case and explains how the Eleventh Circuit's decision in *Compulife* articulated a trade secret theory for data scraping liability. Section IV argues that the *Compulife* decision advances valuable policy interests.

Sections V and VI situate *Compulife* within the broader legal landscape. Data scraping is fundamentally a problem of copying data. IP law—namely, copyright law—typically handles cases involving the copying of information.[20] However, copyright law offers "thin," limited protection for databases, so websites often do not have an actionable copyright claim against scrapers. In other words, copyright law's failure to protect databases has left a gap. To fill this gap, courts and litigators have turned to the CFAA and contract law. These doctrines basically allow websites to assert "quasi-IP" rights in their databases.

Section V argues that the CFAA and contract law are blunt tools for analyzing data scraping cases because they fail to consider IP law norms. These quasi-IP doctrines do not consider the appropriate factors in ascribing liability, and they fail to find the appropriate balance among the competing interests of websites, scrapers, and society. Section VI analyzes how, in the EU, the *sui generis* database right has filled the database gap left by copyright, including in data scraping cases. Section VI then explains how *Compulife* is essentially the U.S.'s attempt to create a *sui generis* database right to fill the database gap left by copyright. Perhaps, *Compulife* signals the U.S.'s recognition of the need for such a right and will usher in a database IP regime much like the EU's legislatively enacted *sui generis* database right.

II. THE DATABASE IP LAW GAP AND THE EMERGENCE OF QUASI-IP

The current IP regime fails to provide website owners with a cognizable legal claim against data scrapers. This Section discusses that doctrinal gap and how it has led website owners to seek recourse through quasi-IP doctrines. Section II.A explains how copyright's failure to protect databases has left a doctrinal gap.

---

[19] *See* E-mail from George W. Jordan III, Chair, American Bar Ass'n, Intell. Prop. Law Section, to Hon. Andrei Iancu, U.S. Under Sec'y of Com. for Intell. Prop. & Dir., U.S. Patent & Trademark Office (Jan. 9, 2020), *available at* https://www.uspto.gov/sites/default/files/documents/ABA-IPL_RFC-84-FR-58141.pdf.

[20] When this Note references IP law alternatives to trade secret law, it is specifically referring to copyright law because data is not patentable. *See* 35 U.S.C. § 101; Diamond v. Chakrabarty, 447 U.S. 303, 309 (1980) ("The laws of nature, physical phenomena, and abstract ideas have been held not patentable.").

Sections II.B through II.D describe how, in the absence of a database IP regime, litigants seeking redress have turned to quasi-IP doctrines—namely, contract law, the CFAA, and state unfair competition law.

A. The Database IP Law Gap Left by Copyright Law

In data scraping cases, "the fundamental disputes are about copying of data."[21] IP doctrines like copyright law typically handle cases involving the copying of information. IP law is well-adapted for such problems because IP law is designed to find the "difficult balance between the interests of [creators] in the control and exploitation of their [works] on the one hand, and society's competing interest in the free flow of ideas, information, and commerce on the other hand."[22] Indeed, the Intellectual Property Clause of the Constitution mandates this careful balance.[23] But while IP law appears to be a natural framework for analyzing data scraping cases, it is woefully inadequate because copyright law gives "thin" protection to databases.

Federal copyright law only protects "original" works.[24] Originality requires "some minimal degree of creativity."[25] One consequence of the originality requirement is that facts by themselves are not copyrightable because they "do[] not 'ow[e] [their] origin' to someone. Rather . . . they existed before [someone] reported them, and would have continued to exist if [someone] had never published [them]."[26] In adopting the "minimal degree of creativity" threshold, the Supreme Court expressly rejected the "sweat of the brow" theory, under which "copyright was a reward for the hard work that went into compiling facts."[27] In its seminal case on the issue, *Feist Publications, Inc. v. Rural Telephone Service Co.*, the Supreme Court denied copyright protection to a telephone directory.[28] Even though the producer expended immense effort to compile the telephone numbers comprising

---

[21] Kathleen C. Riley, Note, *Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 245, 284–85 (2019). In a comprehensive survey of all the data scraping cases decided under the CFAA, Andrew Sellars found that "a tremendous number of these opinions concern claims brought by direct commercial competitors or companies in closely adjacent markets to each other. A far smaller number involve commercial scrapers with noncommercial hosts. Only three opinions involve a commercial data host and a public-interest-oriented scraper." Sellars, *supra* note 15, at 390.

[22] Sony Corp. v. Universal City Studios, 464 U.S. 417, 479 (1984).

[23] *Id.* (interpreting U.S. CONST. ART. I, § 8, cl. 8). Even though federal trade secret law is not based in the Intellectual Property Clauses, it is still driven by the same rationales. *See generally* Mark Lemley, *The Surprising Virtues of Treating Trade Secret Rights as IP Rights*, 61 STAN. L. REV. 311, 329–41 (2008).

[24] 17 U.S.C. § 102.

[25] Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991).

[26] *Id.* at 361. Another rationale for the uncopyrightability of facts is the idea-expression or fact-expression dichotomy. Authors cannot copyright ideas or facts because other authors need to use such ideas and facts to create other works. *Id.* at 350.

[27] *Id.* at 352–61.

[28] *Id.* at 361–64.

the directory, the directory was merely a collection of unoriginal facts, and hence uncopyrightable.[29]

While facts themselves are unprotected, original compilations of facts may be protected. That is, a compilation can be copyrighted if the facts have been "selected, coordinated, or arranged" in an original way."[30] In *Feist*, the facts (the names and telephone numbers) were merely listed alphabetically, so there was no "minimal degree of creativity."[31] If the telephone listings had been arranged in some creative way, they might have achieved copyright protection. However, this protection would have been very "thin" because the "copyright is limited to the particular selection or arrangement. In no event may copyright extend to the facts themselves."[32] For example, had the telephone book arranged the listings to create text art, a competitor could not lawfully copy the artful arrangement but would be free to copy the factual listings.

There is also room to argue that a database contains copyrightable, subjective facts "infused with the author's taste or opinion."[33] For example, ratings—such as Standard & Poor's "Buy" assessment of a stock or Michelin Guide restaurant reviews—are copyrightable.[34] However, this narrow exception is not helpful for websites striving to deliver accurate, up-to-date, objective facts. Indeed, many databases are valuable precisely because their informational contents have been carefully processed and vetted to be as accurate and objective as possible.

Ultimately, databases receive very "thin" protection under copyright law.[35] First, the objective factual content of databases is not copyrightable. A narrow exception exists for subjective facts, but many websites cannot use this exception. Second, while the structure and organization of databases may be copyrighted, this protection does not extend to the data itself.[36]

---

[29] *Id.*

[30] *Id.* at 341 (citing 17 U.S.C. § 101).

[31] *Id.* at 362.

[32] *Id.* at 349–51.

[33] James Grimmelmann, *Three Theories of Copyright in Ratings*, 14 VAND. J. ENT. & TECH. L. 851, 861 (2012) (citing CCC Info. Servs., Inc. v. Maclean Hunter Mkt. Reports, Inc., 44 F.3d 61 (2d Cir. 1994)).

[34] *Id.* at 867–82.

[35] *See* Jane C. Ginsburg, *Copyright, Common Law, and Sui Generis Protection of Databases in the United States and Abroad*, 66 U. CIN. L. REV. 151, 153–57 (1997). Because databases are often unprotected by copyright law, the Digital Millennium Copyright Act's prohibition on circumventing technological copyright protection systems is inapplicable because it only protects copyrightable works. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 549–550 (6th Cir. 2004) (interpreting 17 U.S.C. § 1202).

[36] Typically, scraping copies data and not the arrangement of data. But there may be an edge case where scraping copies the arrangement itself. For example, Westlaw organizes their cases by factors like procedural posture. This arrangement is arguably original. Therefore, a scraper that copies all of the cases with a specific procedural posture may have infringed the copyright in the arrangement.

Copyright law has a database-sized gap. To fill this gap, courts and litigators have turned to the CFAA and contract law as quasi-IP law.[37] But these quasi-IP doctrines fail to (1) provide a workable framework for analyzing data scraping cases and (2) balance the websites' interests in protecting databases with society's interests in the free flow of information.

B. Contract Law as Quasi-IP

In the absence of a database IP regime, litigants have turned to other doctrinal frameworks such as contract law. These alternative frameworks have become quasi-IP, granting rights in databases otherwise unprotected by IP law.

1. Contract Law Claims Against Data Scrapers

A website can assert a contract law claim against a scraper when the website's terms of service prohibit scraping; however, the success of such a claim turns on whether these online contracts are binding. The three main types of online contracts are: clickwrap (where the user must affirmatively click "I agree" before accessing the website), scrollwrap (where the user must scroll through the contract and click "I agree"), and browsewrap (where the user agrees to the contract merely by using the website).[38] Courts have generally found clickwrap and scrollwrap agreements enforceable.[39] The enforceability of browsewrap contracts has turned on whether the user had "actual or constructive knowledge of the terms."[40] If the court finds that the terms of service are a binding contract, the scraper is almost certainly liable because the terms of service will almost invariably prohibit scraping.[41]

---

[37] *See* Nicholas A. Wolfe, *Hacking the Anti-Hacking Statute: Using the Computer Fraud and Abuse Act to Secure Public Data Exclusivity*, 13 NW. J. TECH. & INTELL. PROP. 301, 306 (2015) (describing the CFAA as "a para-copyright tool to secure exclusivity to otherwise publicly accessible data"); Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 324 (2004) ("[T]he CFAA is now being used to control access to and the use of information contained on publicly available websites. Recent court decisions have allowed website owners to utilize the CFAA to override the carefully balanced provisions of the copyright laws."); Jane C. Ginsburg, *A Marriage of Convenience? A Comment on The Protection of Databases*, 82 CHI.-KENT L. REV. 1171, 1172 (2007) (explaining how contract law is quasi-IP law).

[38] Erin Canino, Note, *The Electronic "Sign-in-Wrap" Contract*, 50 U.C. DAVIS L. REV. 535, 539–41 (2016) (citing cases); *see* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) (finding shrinkwrap contract enforceable).

[39] Canino, *supra* note 38, at 539–41.

[40] Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1176 (9th Cir. 2014).

[41] *See* Casey Fiesler, Nathan Beard, & Brian C. Keegan, *No Robots, Spiders, or Scrapers: Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service*, 14 PROCS. INT'L AAAI CONF. WEB & SOC. MEDIA 187, 191 (2020) (finding 80% of social media websites ban scraping in their terms of service); *see, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 398–404 (2d Cir. 2004) (awarding preliminary injunction for website's terms of service claim); Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654HLH(BQRx), 2003 WL 21406289, at *1–

By placing terms of service on its website, a plaintiff gains the right to prevent copying, transforming its database into a form of intellectual property.[42] Indeed, browsewrap contracts that are enforceable against anyone who visits the website resemble property rights enforceable against the world at large.[43] But while contract law provides websites with quasi-IP rights in their databases, contract law has none of the IP policy levers copyright law has. For example, contract law has no fair use defense, does not examine the fair competition issues implicated by scraping, and does not inquire into whether the website's database is even worthy of protection. Contract law only looks at whether the terms of service are binding—whether users have notice of the terms of service.[44]

2. The Failures of Contract Law as Quasi-IP

Contract law places undue emphasis on the existence of a contract, making it an inappropriate framework to analyze data scraping. In considering terms of service contract claims, courts are unable to consider factors such as whether the data should be protected under a Lockean labor theory or the purposes of scraping.[45] Instead, courts simply look at whether the terms of service were a contract; if the terms are binding, then the scraper is liable.[46] And, in many cases, the contract question boils down to whether the scraper had notice.[47] Thus, scraping liability under contract law amounts to whether the scraper had notice of the contract. Moreover, accepting a terms of service argument may have problematic ramifications for contract law given the unfairness of clickwrap, scrollwrap, and browsewrap contracts.[48] Ultimately, drawing the line between lawful and unlawful scraping on the basis of a contract that no one reads is an arbitrary and unfair rule.

Using browsewrap agreements to prohibit scraping also elides the distinction between property and contract law. Judicial enforcement of browsewrap contracts "erode[s] the distinction between *inter-partes* contract rights and *erga-omnes*

---

2 (C.D. Cal. Mar. 7, 2003) (denying scraper's motion for summary judgment on website's terms of service claim).

[42] *See* Ginsburg, *supra* note 35, at 167–71 (explaining how contract law is quasi-IP).

[43] *See* Ginsburg, *supra* note 37, at 1172.

[44] *See Nguyen*, 763 F.3d at 1176 (analyzing whether browsewrap contract was binding).

[45] Perhaps, the scraper could argue that enforcement of the terms of service as a binding contract violates public policy (e.g., IP law norms, antitrust law norms). *See generally* David A. Friedman, *Bringing Order to Contracts Against Public Policy*, 39 FLA. ST. U. L. REV. 563 (2012).

[46] *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 398–404 (2d Cir. 2004) (awarding preliminary injunction for website's terms of service claim); Sw. Airlines Co. v. Roundpipe, LLC, 375 F. Supp. 3d 687, 706 (N.D. Tex. 2019) (rejecting motion to dismiss website's terms of service claim).

[47] *See Nguyen*, 763 F.3d at 1176.

[48] *See generally* Charles E. MacLean, *It Depends: Recasting Internet Clickwrap, Browsewrap, I Agree, and Click-through Privacy Clauses as Waivers of Adhesion*, 65 CLEV. ST. L. REV. 43 (2017) (arguing such contracts are unenforceable contracts of adhesion).

property rights."[49] If browsewrap contracts grant the website an exclusionary right against the world (i.e., an intellectual property right), why not reframe the data scraping issue in terms of intellectual property law? If it looks like IP, walks like IP, and quacks like IP, it probably is IP.

C. Computer Fraud and Abuse Act ("CFAA") as Quasi-IP

In the absence of an IP database regime, litigants have also turned to the CFAA—an anti-hacking statute premised on criminal trespass principles—to protect their interests in databases.

1. CFAA Claims Against Data Scrapers

Under the CFAA, "[w]hoever . . . intentionally accesses a computer *without authorization* or *exceeds authorized access* . . . and thereby obtains . . . information from any protected computer . . . shall be" liable.[50] While the CFAA is principally a federal criminal statute, it also provides a private right of action to "[a]ny person who suffers damage or loss [greater than $5,000]."[51]

CFAA liability rests on the interpretations of "without authorization" and "exceeds authorized access." The two dominant interpretation methodologies are the narrower, code-based interpretation and the broader, contract-based interpretation.[52] Under the code-based interpretation, a scraper is liable if it has circumvented technological access barriers.[53] For example, scraping that bypasses a login password violates the CFAA.[54] The contract-based interpretation is much broader.[55] Under the contract-based interpretation, a scraper is liable if it has circumvented technological access restrictions as well as non-technological access

---

[49] Ginsburg, *supra* note 37, at 1172; *see also* Ginsburg, *supra* note 35, at 167 ("The classic distinction between a contract right *inter partes* and a property right *erga omnes* dissolves when all users must become the information provider's co-contractants.").

[50] 18 U.S.C. § 1030(a)(2)(C) (emphasis added). A "protected computer" is a computer "used in or affecting interstate or foreign commerce or communication," which is any computer connected to the Internet. 18 U.S.C. § 1030(e)(2)(B); United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (noting that "protected computer" refers to "all computers with Internet access"). "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

[51] 18 U.S.C. § 1030(g).

[52] Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1455–60 (2016); Orin S. Kerr, *Cybercrime's Scope*, 78 N.Y.U. L. REV. 1596, 1645–46 (2003).

[53] Bellia, *supra* note 52, at 1457–60.

[54] Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 933–35 (9th Cir. 2004) (bypassing password login was CFAA violation); *cf.* United States v. Nosal, 844 F.3d 1024, 1036 (9th Cir. 2016) (holding that using someone else's password violated the CFAA); Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) (holding that accessing an "unprotected public communications system[]" did not violate the CFAA).

[55] Bellia, *supra* note 52, at 1455–57.

restrictions (i.e., verbal and contractual restrictions) such as a cease-and-desist letter[56] or a terms of service agreement.[57] Courts have uniformly adopted the code-based interpretation.[58] But, there is substantial disagreement over the acceptability of the contract-based interpretation.[59] Tricky edge cases, such as bypassing CAPTCHAs and password sharing, also blur the distinction between code-based and contract-based restrictions.[60] Further, difficult cases, such as Internet Protocol address blocking, stress the limits of the code-based interpretation.[61]

The recent Supreme Court case *Van Buren v. United States*—the Supreme Court's first and only case analyzing the CFAA—narrowed the interpretation of "exceeds authorized access" by rejecting a purpose-based interpretation, but failed to definitively adopt either the code-based or contract-based interpretation of "authorization."[62] In *Van Buren*, the government prosecuted a police officer, who improperly accessed a license plate database in exchange for payment, on the theory that—while he had authorized access via his username and password login—he "exceed[ed] authorized access" by accessing the database for an improper purpose.[63] The *Van Buren* Court rejected the government's purpose-based interpretation, holding that the CFAA "does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them."[64] According to the Court, "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off

---

[56] *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1065 (9th Cir. 2016) (bypassing cease-and-desist letter was CFAA violation); Craigslist v. 3Taps, 964 F. Supp. 2d 1178, 1181–87 (N.D. Cal. 2013) (bypassing IP blocking and cease-and-desist letter was CFAA violation).

[57] *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (violating employer policy prohibiting using database for personal purposes was CFAA violation).

[58] Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner, United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (U.S. Apr. 20, 2020) (No. 19-783), 2020 WL 4003433, at *5 ("Importantly, no one disputes that the CFAA criminalizes this kind of access . . . everyone agrees that the CFAA criminalizes the bypassing of code-based restrictions.").

[59] PETER G. BERRIS, CONG. RSCH SERV., CYBERCRIME AND THE LAW: COMPUTER FRAUD AND ABUSE ACT (CFAA) AND THE 116TH CONGRESS, 24–26 (2020), *available at* https://fas.org/sgp/crs/misc/R46536.pdf.

[60] Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233, 254 (2010) ("CAPTCHA [] is really just a code-based barrier implementing a contract-based restriction—namely, one prohibiting the use of 'bots' on a website."); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1178–80 (2016) (analyzing password sharing).

[61] Craigslist, Inc. v. 3Taps, Inc., 964 F. Supp. 2d 1178, 1181–87 (N.D. Cal. 2013) (holding circumvention of Internet Protocol address blocking to be violation of CFAA); Kerr, *supra* note 60, at 1167–68 (arguing that *Craigslist* was wrong because an Internet Protocol address block "is not a real barrier").

[62] Van Buren v. United States, 141 S. Ct. 1648 (2021).

[63] *Id.* at 1653–54.

[64] *Id.* at 1652.

limits to him."[65] In its analysis, the *Van Buren* Court adopted a "gates-up-or-down" analogy.[66] According to the Court, to violate the CFAA's prohibition on "access without authorization" or "exceed[ing] authorized access," a person must bypass a "gate" that the person is not authorized to bypass (i.e., an "up" gate).[67] Still, the Court did not clarify what exactly constitutes an "up" gate—the Court refused to clarify which of the code-based or contract-based interpretation of "authorization" is correct—leaving the CFAA as ambiguous as ever.[68]

In *hiQ v. LinkedIn*, the Ninth Circuit applied *Van Buren* to reject LinkedIn's attempt to use the CFAA to prevent the scraping of public LinkedIn profiles.[69] While LinkedIn implemented access restriction measures such as Internet Protocol address blocking, a terms of service prohibiting scraping, and a cease and desist letter, the court found these restrictions insufficient to trigger the CFAA.[70] In its analysis, the Ninth Circuit adopted a strict code-based interpretation, interpreting "without authorization" to mean "when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer."[71] According to the court, the "gates" were down because the public LinkedIn profiles were "presumptively open to all comers."[72] "Where, as here, prior authorization is not generally required, but a particular person—or—bot is refused access," the CFAA does not apply.[73] The Ninth Circuit's interpretation of *Van Buren* and the CFAA adopted a strict code-based interpretation; however, because of the ambiguity left open by the Supreme Court, other circuits may adopt different approaches.

Ultimately, by placing technological or, possibly, contractual access restrictions on its website, a plaintiff can transform its database into intellectual property, gaining the power to prevent copying.[74] Just like contract law, the CFAA creates a quasi-IP regime.[75] And just like contract law, the CFAA does not have the IP law toggles that copyright has.[76] The CFAA simply looks at whether the website had

---

[65] *Id.* at 1662.

[66] *Id.* at 1658–59.

[67] *Id.*

[68] *Id.* at 1659 n.8 ("For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies.").

[69] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1187 (9th Cir. 2022).

[70] *Id.* at 1187–88.

[71] *Id.* at 1201.

[72] *Id*. at 1199.

[73] *Id.* at 1195.

[74] *See* Wolfe, *supra* note 37, at 306 (describing the CFAA as "a para-copyright tool to secure exclusivity to otherwise publicly accessible data").

[75] *See generally* Charles Duan, *Hacking Antitrust: Competition Policy and the Computer Fraud and Abuse Act*, 19 COLO. TECH. L.J. 313, 337–38 (2021) (describing the CFAA as an "ad hoc 'copyright' regime").

[76] *See supra* notes 42–44 and accompanying text.

technological or contractual access restrictions and whether the scraper circumvented those restrictions.

2. The Failures of the CFAA as Quasi-IP

Courts apply the CFAA by analogizing to criminal trespass law.[77] As the 1984 House Report on the CFAA explained, "the conduct prohibited [under the CFAA] is analogous to that of 'breaking and entering.'"[78] For example, Professor Orin Kerr argues that courts should analyze CFAA liability using "norms of computer trespass," just like how criminal trespass law looks at "physical trespass norms."[79] Specifically, Professor Kerr argues that the CFAA analysis should look at three factors to inform these trespass norms: (1) the nature of the space (e.g., in the physical world, it would be considered trespass to enter a private home, but not trespass to enter a public mall);[80] (2) the means of access (e.g., permission to enter is limited to specific methods of entrance; it is understood one can enter a store via the front door, but not by jumping through an open window);[81] and (3) the context of access (e.g., keys are a legal means of access, but finding a lost key does not create permission to use that key to open the front door).[82]

Professor Kerr's theory of trespass norms helps elucidate the CFAA's concept of unauthorized access. For example, Professor Kerr's theory can be applied to CFAA edge cases like circumventing CAPTCHAs and password sharing.[83] However, application of the CFAA and trespass law norms to data scraping cases means that CFAA liability turns on the mere act of "entering" the website rather than on IP norms such as whether the data even qualifies for anti-copying protection in the first place.[84] The Ninth Circuit aptly summarized that "the CFAA is best understood as an anti-intrusion statute and not as a 'misappropriation statute.'"[85] Under the CFAA, scraping a unique database that took thousands of hours to create is identical to scraping a database that parrots what already exists in the public

---

[77] Kerr, *supra* note 60, at 1159 ("It is worth asking whether trespass provides the right framework to apply . . . I think the answer [is] . . . yes. Trespass provides an appropriate framework."); *see also* Laurent Sacharoff, *Criminal Trespass and Computer Crime*, 62 WM. & MARY L. REV. 1 (2020) (applying trespass law norms to CFAA); Josh Goldfoot & Aditya Bamazai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1483 (2016) (same).

[78] H.R. Rep. No. 98-894, at 20 (1984).

[79] Kerr, *supra* note 60, at 1148–53.

[80] *Id.* at 1148–50.

[81] *Id.* at 1150–52.

[82] *Id.* at 1152–53.

[83] *Id.* at 1169–70 (CAPTCHA analysis); *id.* at 1178–80 (password sharing analysis).

[84] *See* Riley, *supra* note 21, at 279–90 (discussing how IP law, specifically copyright law, is the proper way to frame data scraping cases).

[85] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1196 (9th Cir. 2022) (citing United States v. Nosal, 676 F.3d 854, 857–58 (9th Cir. 2012)).

domain.[86] The CFAA's failure to distinguish between these two cases is a fatal flaw because at the core of data scraping is the data being copied. In terms of a physical analogy, data scraping is wrong not because an intruder entered your home (i.e., your website) but because that intruder took valuable property (i.e., data) from your home.[87] Similarly, in the eyes of the CFAA, scraping for nonprofit research purposes is identical to scraping that is free-riding.[88] The CFAA fails to recognize that data scraping for certain purposes may override any proprietary interests in the data; meanwhile, copyright law recognizes this concept as the fair use doctrine.

In sum, because the CFAA does not consider IP law norms, "it protects information but lacks the competition-protective features of [IP law.] [T]he CFAA essentially creates an ad hoc intellectual property regime that enables the improper suppression of competition."[89] Furthermore, even if courts want to consider IP factors such as what kind of data was scraped and the purposes of scraping, statutory interpretation principles may prevent courts from considering such extratextual factors.[90]

Scholars have also criticized the CFAA as unconstitutionally vague and overbroad.[91] Finding data scrapers liable under the CFAA may broaden the interpretation of the CFAA and sweep otherwise lawful and socially beneficial activities within the ambit of the CFAA.[92] For example, courts interpreting the CFAA to prohibit circumvention of contract-based restrictions effectively make it a federal crime to violate cease-and-desist letters (which can be empty threats with

---

[86] *See* Duan, *supra* note 75, at 331 ("[The] discrepancies between the CFAA and intellectual property regimes, specifically information that is protected under the CFAA but specifically excluded from intellectual property, are revealing as to competition concerns with the CFAA, because exclusions from intellectual property protections generally reflect legislative judgments about competition policy."); Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. 155, 157 (2008) (Some cases have involved theft of computer-stored trade secrets. In these cases, plaintiffs have alleged CFAA violations in addition to (or as substitutes for) trade secret claims. Because the CFAA hinges on access, it "protects all valuable computer data regardless of whether it is proven a trade secret under state law.").

[87] *See* RESTATEMENT (SECOND) OF TORTS § 158 (AM. L. INST. 1965) ("One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally (a) *enters* land in the possession of the other. . . .") (emphasis added) [hereinafter RESTATEMENT (SECOND) OF TORTS].

[88] Some courts have considered whether a First Amendment exception to the CFAA applies to excuse scraping for research purposes; however, this is far from settled law. *See* Sandvig v. Barr, 451 F. Supp. 3d 73 (D.D.C. 2020) (not reaching the First Amendment question).

[89] Duan, *supra* note 75, at 313–14.

[90] *See* Bostock v. Clayton County, 140 S. Ct. 1731, 1737 (2020) ("[W]hen the express terms of a statute give us one answer and extratextual considerations suggest another, it's no contest. Only the written word is the law.").

[91] Sacharoff, *supra* note 77, at 17–20; Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563 (2010).

[92] *See* Brief of Professor Orin S. Kerr, *supra* note 58, at *9–13 ("Extending CFAA Liability to Contract-Based Violations Would Lead to Astonishing Results.").

no firm legal bases) and terms of service provisions.[93] This is especially problematic because prosecutors have been accused of misusing the CFAA by being overly aggressive.[94]

D. State Unfair Competition Law as Quasi-IP

Finally, plaintiffs may bring various unfair competition claims, such as common law misappropriation ("hot news" tort),[95] unjust enrichment,[96] conversion,[97] and trespass to chattel.[98]

1. State Unfair Competition Law Claims Against Data Scrapers

The "hot news" tort originated with the seminal Supreme Court case *INS v. AP*. There, the wire service agency International News Service copied the facts reported in the news bulletins of its competitor Associated Press. While facts in news were otherwise uncopyrightable information in the public domain, the Supreme Court recognized that these facts were "the result of organization and the expenditure of labor, skill, and money" and that INS was "endeavoring to reap where it has not sown."[99] As such, the Court held that AP had so-called "*quasi*-property" interests in the factual content of news and a right to redress against INS.[100]

Modern courts have fleshed out the reasoning in *INS* to create the "hot news" tort, wherein:

> (i) the plaintiff generates or collects information at some cost or expense; (ii) the value of the information is highly time-sensitive; (iii) the defendant's use of the information constitutes free-riding on the plaintiff's costly efforts to generate or collect it; (iv) the defendant's use of the information is in direct competition with a product or service

---

[93] *See EFF To Supreme Court: Violating Terms of Service Isn't a Crime Under the CFAA*, ELECTRONIC FRONTIER FOUNDATION (July 8, 2020), https://www.eff.org/press/releases/eff-asks-supreme-court-rule-violating-terms-service-isnt-crime-under-cfaa.

[94] Like the CFAA, trade secret law has a criminal component in addition to a civil component. *See* 18 U.S.C. § 1831. However, prosecutors have not overreached in trade secret cases as they have in CFAA cases. *See* Austin C. Murnane, *Faith and Martyrdom: The Tragedy of Aaron Swartz*, 24 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1101 (2015) (telling the tragic story of Aaron Swartz, who, after being prosecuted under the CFAA for downloading academic articles, committed suicide); United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (vacating jury verdict against Lori Drew who was prosecuted under the CFAA for cyberbullying).

[95] *See, e.g.*, Allure Jewelers, Inc. v. Ulu, No. 1:12CV91, 2012 WL 4322519 (S.D. Ohio Sept. 20, 2012).

[96] *See, e.g.*, Snap-on Bus. Sols. Inc. v. O'Neil & Assocs., Inc., 708 F. Supp. 2d 669, 680–82 (N.D. Ohio 2010); ShopLocal LLC v. Cairo, Inc., No. CIV.A. 05 C 6662, 2006 WL 495942, at *3 (N.D. Ill. Feb. 27, 2006).

[97] *See, e.g.*, QVC, Inc. v. Resultly, LLC, 159 F. Supp. 3d 576 (E.D. Pa. 2016).

[98] *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1065–71 (N.D. Cal. 2000).

[99] Int'l News Serv. v. Associated Press, 248 U.S. 215, 247 (1918).

[100] *Id.*

> offered by the plaintiff; (v) the ability of other parties to free-ride on the efforts of the plaintiff would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened.[101]

Two other closely related state law torts are conversion and trespass to chattel. These two doctrines "are essentially the same [as each other]. The difference is that conversion entails a more serious deprivation of the owner's rights such that an award of the full value of the property is appropriate."[102] "A trespass to a chattel may be committed by intentionally . . . using or intermeddling with a chattel in the possession of another" such that "the chattel is impaired as to its condition, quality, or value, or . . . the possessor is deprived of the use of the chattel for a substantial time."[103] Initially, courts took an expansive view of the actual injury requirement. In *eBay v. Bidder's Edge*, the court held that data scraping was actionable under a trespass to chattel theory because the scraping bot sent requests to the plaintiff's computer systems, which took "valuable bandwidth and capacity and necessarily compromis[ed] eBay's ability to use that capacity for its own purposes," even though the scraping requests amounted to less than two percent of eBay's total bandwidth.[104] In *Oyster Software, Inc. v. Forms Processing, Inc.*, the court interpreted *eBay* to hold that physical interference with the plaintiff's computers was unnecessary—mere "use" of the plaintiff's computers was sufficient.[105]

However, the California Supreme Court in *Intel Corp. v. Hamidi* dramatically constricted the scope of trespass to chattel.[106] In *Intel*, a former Intel employee sent millions of spam emails to Intel email addresses, and Intel sought to recover on a trespass to chattels theory. The *Intel* Court rejected the broad reasoning of *eBay* and *Oyster*, holding that Intel had to "demonstrate some measurable loss from the use of its computer system [by the defendant]."[107]

2. The Failures of State Unfair Competition Law as Quasi-IP

These state unfair competition law doctrines come closer than contract law and the CFAA to recognizing the IP nature of and the unfair competition principles underpinning data scraping. Indeed, the Supreme Court aptly foreshadowed this development in *INS v. AP* when it coined the term "*quasi*-property" to describe AP's property interest in otherwise uncopyrightable factual news.[108] Still, these

---

[101] Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 852–53 (2d Cir. 1997) (citing Int'l News Serv. v. Associated Press, 248 U.S. 215 (1918).

[102] QVC, Inc. v. Resultly, LLC, 159 F. Supp. 3d 576, 599 (E.D. Pa. 2016).

[103] RESTATEMENT (SECOND) OF TORTS §§ 217(b), 218(b)–(c).

[104] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

[105] Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382, at *13 (N.D. Cal. Dec. 6, 2001).

[106] Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1350–51 (2003).

[107] *Id.*

[108] Int'l News Serv. v. Associated Press, 248 U.S. 215, 248 (1918) (emphasis in original).

doctrines fail to properly capture the full breadth of data scraping cases because these doctrines only exist in very narrow circumstances.

The "hot news" tort only protects time-sensitive information, leaving a wide variety of databases unprotected. Likewise, to prove conversion or trespass to chattel, a plaintiff must meet a stringent standard of showing actual injury to its computer systems. In many cases, scraping will have a negligible impact on the plaintiff's servers, making a conversion or trespass to chattel claim unlikely to succeed.[109]

* * *

Given the inadequacies of contract law, the CFAA, and state unfair competition law to provide a framework for data scraping, can another area of law help fill the database gap left open by copyright law? Section III explains how *Compulife* and trade secret law provide an answer.

III. *COMPULIFE* CREATED A TRADE SECRET CAUSE OF ACTION FOR DATA SCRAPING

At first blush, trade secret law seems inapplicable to data scraping: the defining feature of a trade secret is secrecy, so how can publicly available (and hence scrape-able) information be secret? This Section explains how *Compulife* created a trade secret cause of action and argues that *Compulife*'s seemingly bizarre holding is reconcilable with trade secret jurisprudence.

Section III.B describes the two prongs of a trade secret claim: (1) the existence of a trade secret and (2) acquisition of the trade secret by "improper means." Section III.C examines *Compulife*'s analysis of the first prong and argues that even if a database is publicly accessible (and hence scrape-able), it can satisfy the secrecy requirement. Section III.C further explains how the "independent economic value" requirement of trade secret law imposes an important limitation on the scope of *Compulife*'s first prong. Section III.D examines *Compulife*'s analysis of the second prong, explaining that courts have broad discretion under trade secret law to find conduct "improper." To guide this discretion, Section III.D proposes principles for courts to use in applying *Compulife*. Finally, Section III.E summarizes the elements for a *Compulife* trade secret claim.

A. Facts of Compulife

In *Compulife*, the plaintiff Compulife created a publicly available website that allowed consumers to request free insurance quotes.[110] At the time of litigation, a user would input her data into the quote generator shown in Figure 1. The website would then return approximately forty quotes, an example of which is shown in

[109] *See* Ticketmaster Corp. v. Tickets.com, Inc., No. 99CV7654, 2000 WL 1887522, at *4 (C.D. Cal. Aug. 10, 2000), *aff'd*, 2 F. App'x 741 (9th Cir. 2001) (rejecting trespass to chattel claim for failure to show actual injury).

[110] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1297 (11th Cir. 2020).

Figure 2, allowing the user to pick the insurance quote most suitable for her.[111] Importantly, Compulife's website was completely public—it did not have technological access (e.g., password authentication) or contractual (e.g., terms of service) restrictions.[112]

Underlying this website was the plaintiff's "Transformative Database," which supplied all the data to run the quote generator. Compulife created the database by applying a "proprietary calculation technique."[113] In addition to providing access to the database via the free website, the plaintiff sold encrypted, stand-alone PC copies of the database to individual insurance agents.[114]

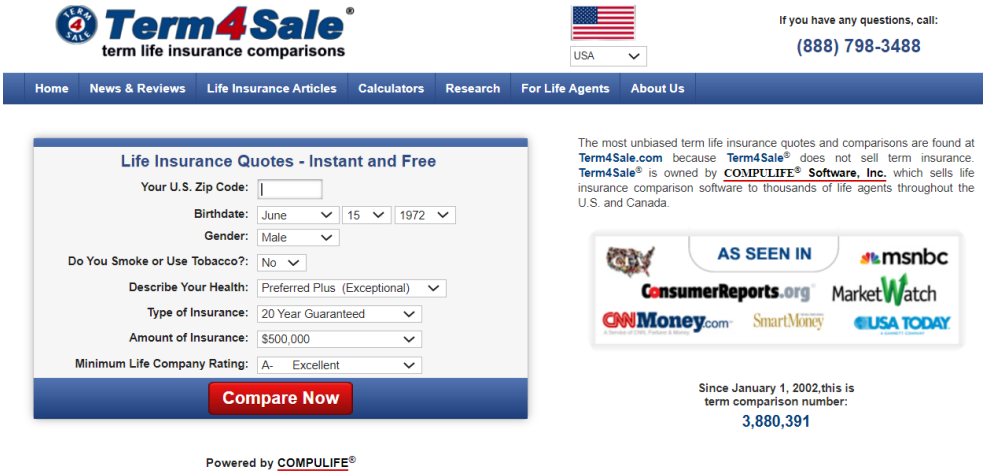

Figure 1. The plaintiff Compulife's website.[115]

---

[111] *Id.* at 1299.

[112] *Id.* at 1317–18 (noting that plaintiff's website did not have any technological access restrictions); Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808-JMH, 2018 WL 11033483, at *11, *6 (S.D. Fla. Mar. 12, 2018) (The district court noted that the scraping occurred between September 1, 2016 and September 6, 2016. "After September 6, 2016, Compulife added a 'Terms of Use Agreement' to the www.term4sale.com website."), *aff'd in part, vacated in part sub nom.*, *Compulife*, 959 F.3d 1288.

[113] *Compulife*, 959 F.3d at 1298.

[114] *Id.* at 1296–97.

[115] WAYBACK MACHINE, https://web.archive.org/web/20160408192942/http://www.term4sale.com/ (Snapshot dated June 28, 2016. The scraping occurred between September 1 and September 6, 2016.).

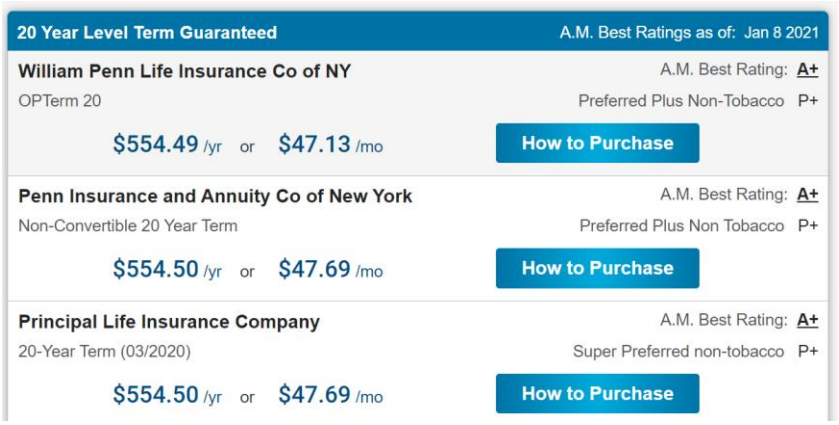

Figure 2. Example of the insurance quotes that the defendant scraped from Compulife.[116]

The defendant, a competing insurance quote website, used a data scraping bot to generate 800,000 unique combinations of input data to scrape 43 million quotes from the plaintiff's website, recreating a significant portion of the plaintiff's database of insurance quotes.[117] The defendant then used the scraped data on its own website.[118] Here, scraping enabled the defendant to offer an identical competing product, which is shown in Figure 3, without having to expend its own resources to create a database.

Figure 3. The defendant used the scraped data to run its competing website.[119]

---

[116] TERM4SALE, https://www.term4sale.com/apit4s/template.php (last visited Jan. 8, 2021).

[117] *Compulife*, 959 F.3d at 1296–97.

[118] *Id.* at 1300.

[119] BEYONDQUOTES, https://www.beyondquotes.com/ (last visited Jan. 8, 2021); *see also* Compulife Software, Inc. v. Newman, No. 9:16-cv-81942 (S.D. Fla. Dec 2, 2016), ECF No. 203, Plaintiff's Exhibit No. 166 (Trial court evidence containing screenshot of defendant's website.).

Notably, the Compulife website had neither a terms of service[120] nor any technological access barriers,[121] meaning Compulife was unable to assert a contract law or CFAA claim. Instead, the plaintiff brought a trade secret claim.

B. Overview of Trade Secret Law

A trade secret claim has two elements: (1) the existence of a trade secret and (2) misappropriation of the trade secret by "improper means."[122] For the first prong, (i) a trade secret must be secret (not "generally known to" and not "readily ascertainable by" others), (ii) the owner must have "taken reasonable measures to keep such information secret," and (iii) "the information [must] derive[] independent economic value" from being secret.[123] The second prong—acquisition by "improper means"—includes acquiring the trade secret by unlawful means such as theft, bribery, misrepresentation, and espionage.[124] However, "improper means" is broad enough to also include acquisition by otherwise legal conduct.[125]

There are two sources of trade secret law: state law and the recently enacted federal Defend Trade Secrets Act ("DTSA").[126] In 48 states (including Florida where *Compulife* was litigated), state trade secret law is modeled on the Uniform Trade Secrets Act ("UTSA").[127] Many courts, including the Eleventh Circuit in *Compulife*, have assumed that the DTSA is "largely identical" to the UTSA and state law.[128] The DTSA's legislative history supports this model of equivalency, explaining that the DTSA "is modeled on the Uniform Trade Secrets Act . . . and

---

[120] Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808-JMH, 2018 WL 11033483, at *6, *11 (S.D. Fla. Mar. 12, 2018) (The scraping occurred between September 1, 2016 and September 6, 2016. "After September 6, 2016, Compulife added a 'Terms of Use Agreement' to the www.term4sale.com website.").

[121] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1317–18 (11th Cir. 2020).

[122] *See* 18 U.S.C. §§ 1839(3), (5); UNIF. TRADE SECRETS ACT (1985) §§ 1(2), (4) (UNIF. LAW COMM'N 1985) [hereinafter UTSA]; RESTATEMENT (FIRST) OF TORTS § 757 (AM. L. INST. 1939) [hereinafter RESTATEMENT (FIRST) OF TORTS]; RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (AM. L. INST. 1995) [hereinafter RESTATEMENT (THIRD) OF UNFAIR COMPETITION].

[123] 18 U.S.C. § 1839(3)(A)–(B); USTA § 1(4).

[124] 18 U.S.C. § 1839(6); USTA (1985) § 1(2).

[125] *See* E. I. du Pont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970) (taking aerial photographs actionable as trade secret misappropriation).

[126] Congress enacted the Defend Trade Secrets Act in 2016. Pub. L. No. 114-153, 130 Stat. 376 (2016) (codified as amended at 18 U.S.C. §§ 1836–1839 (2016)).

[127] *Trade Secrets Act*, UNIFORM LAW COMMISSION, https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 (last visited Jan. 20, 2021) (New York and North Carolina have not adopted the UTSA.).

[128] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1310 n.13 (11th Cir. 2020); Danielle A. Duszczyszyn & Daniel F. Roland, *Three Years Later: How the Defend Trade Secrets Act Complicated the Law Instead of Making It More Uniform*, n.14, FINNEGAN (Aug. 2019), https://www.finnegan.com/en/insights/articles/three-years-later-how-the-defend-trade-secrets-act-complicated-the-law-instead-of-making-it-more-uniform.html (collecting cases).

offers a complementary Federal remedy [to state trade secret law] if the [federal] jurisdictional threshold . . . is satisfied."[129]

C. Prong 1: Existence of a Trade Secret

1. The Eleventh Circuit's Decision

The *Compulife* district court found the database to be a trade secret because it was not easily replicable using public information and because the plaintiff maintained its secrecy through security features, including encrypting the database when selling it to individual insurance agents.[130] Because the plaintiff did not appeal the district court's finding that the database was a trade secret, the Eleventh Circuit did not actually rule on this prong. Nevertheless, the Eleventh Circuit suggested that it would not have overruled the district court's finding.[131] In so holding, the Eleventh Circuit distinguished the individual pieces of data, which are not trade secrets, from the complete database, which is a trade secret:

> The [lower court] was correct to conclude that the scraped quotes [i.e., the data] were not *individually* protectable trade secrets because each is readily available to the public—but that doesn't in and of itself resolve the question whether, in effect, the database *as a whole* was misappropriated. Even if quotes [individual pieces of data] aren't trade secrets, taking enough of them must amount to misappropriation of the underlying secret [i.e., the database] at some point. Otherwise, there would be no substance to trade-secret protections for "compilations," which the law clearly provides.[132]

The striking feature of the Eleventh Circuit's analysis is that it seems to diverge from the *sine qua non* of trade secret law—secrecy.[133] The Compulife website had no restrictions on scraping: it had no password login requirement, CAPTCHAs, nor even a terms of service prohibiting scraping. The database was freely accessible through the public website, yet the Eleventh Circuit was willing to find (and the district court indeed found) the database to be a trade secret. But, "can publicly

---

[129] H.R. REP. NO. 114-529, at 5 (2016); *see id.* at 14 (noting the DTSA "is not intended to alter the balance of current trade secret law or alter specific court decisions" on misappropriation); S. REP. NO. 114-220, at 10 (2016) (same); 18 U.S.C. § 1838 ("[T]his chapter [the DTSA] shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret . . . .").

[130] Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808-JMH, 2018 WL 11033483, at *18–22 (S.D. Fla. Mar. 12, 2018).

[131] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1311 (11th Cir. 2020) ("The magistrate judge found that Compulife's Transformative Database was a trade secret, a finding that is not clearly erroneous and that, in any event, does not seem to be contested on appeal.").

[132] *Id.* at 1314 (emphasis in original).

[133] *Id.* at 1315 ("[T]he simple fact that the quotes taken were publicly available does not automatically resolve the question in the defendant's favor.").

available data be a trade secret?"[134] One commentator answered this with a resounding no, calling *Compulife* "contrary to a basic understanding of trade secret law" because information "freely accessible to the public" cannot be a trade secret.[135] Section III.C.2 addresses these critiques and explains how a database can be a trade secret even when its data is public. Then, Section III.C.3 explains the "independent economic value" requirement.

2. Data Is Public, but the Underlying Database Is Secret

Above all else, a trade secret must be secret.[136] In *Compulife*, the Eleventh Circuit made the crucial analytical distinction between individual pieces of data and the underlying database.[137] While *individual* pieces of data are not secret, the database *as a whole* is. This distinction between the parts and the whole is well-established in trade secret law, as compilations of information are protectable even when each piece of information is public knowledge. The Restatement (Third) of Unfair Competition explains: "It is the secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation or integration of the individual elements."[138] For example, in *AirFacts, Inc. v. de Amezaga*, the Fourth Circuit held that flowcharts organizing publicly available information were trade secrets.[139] The Fourth Circuit explained that these flowcharts deserved protection because the "painstaking, expert arrangement of the [public] data made the flowcharts inherently valuable separately and apart from the publicly available contents . . . . [The flowcharts] succinctly display the vast

---

[134] Kieran McCarthy, *A Closer Look at a Troubling Anti-Scraping Ruling from Spring—Compulife Software v. Newman (Guest Blog Post)*, TECHNOLOGY & MARKETING LAW BLOG (Sept. 14, 2020), https://blog.ericgoldman.org/archives/2020/09/a-closer-look-at-a-troubling-anti-scraping-ruling-from-spring-compulife-software-v-newman-guest-blog-post.htm (criticizing *Compulife*).

[135] Peter J. Toren, *A Dubious Decision: Eleventh Circuit Finds Scraping of Data from a Public Website Can Constitute Theft of Trade Secrets (Part I)*, IPWATCHDOG (July 2, 2020), https://www.ipwatchdog.com/2020/07/02/dubious-decision-eleventh-circuit-finds-scraping-data-public-website-can-constitute-theft-trade-secrets-part/id=123029/ (criticizing *Compulife*).

[136] *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39.

[137] The Eleventh Circuit stated: "The [lower court] was correct to conclude that the scraped quotes [i.e., the data] were not individually protectable trade secrets because each is readily available to the public—but that doesn't in and of itself resolve the question whether, in effect, the database as a whole was misappropriated. Even if quotes [individual pieces of data] aren't trade secrets, taking enough of them must amount to misappropriation of the underlying secret [i.e., the database] at some point. Otherwise, there would be no substance to trade-secret protections for 'compilations,' which the law clearly provides." *Compulife*, 959 F.3d at 1314 (emphasis in original); *see also* UAB "Planner5D" v. Facebook, Inc., No. 19-CV-03132-WHO, 2020 WL 4260733, at *1 (N.D. Cal. July 24, 2020) (making a similar distinction between public-facing data and "underlying data files" and finding that trade secrets can subsist in the underlying files).

[138] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f; *see also* 1 MELVIN F. JAGER, *Trade Secrets Law* § 5:28 (2020).

[139] AirFacts, Inc. v. de Amezaga, 909 F.3d 84, 97 (4th Cir. 2018).

amounts of [public] data."[140] Just like the flowcharts in *AirFacts*, databases derive independent economic value as compilations of data. The systematic organization of disparate pieces of information is immensely valuable, driving a $300 billion data industry.[141] Indeed, Compulife made substantial revenue from selling stand-alone PC versions of its database.[142]

Nevertheless, while the data may be public, the underlying database must actually be secret. The standard for determining secrecy is relative secrecy, not absolute secrecy. As the Restatement (Third) of Unfair Competition explains, secrecy "need not be absolute . . . . [T]he requirement of secrecy is satisfied if it would be difficult or costly for others who could exploit the information to acquire it without resort to wrongful conduct."[143] For example, courts have found software source code to be protectable trade secrets, even when the compiled source code—the object code—is widely distributed.[144] When analyzing whether a database is secret, the court should ask whether the database *as a whole* is generally known to others. If it is not, then the database is secret. In any event, because the relative secrecy standard is so flexible, courts have significant discretion to hold that information is sufficiently secret to be a trade secret.[145]

Moreover, a website's decision to place its database on the Internet and allow public access to individual pieces of data does not mean that the website failed to take "reasonable measures to keep [its database] secret."[146] As the Eleventh Circuit explained, "while Compulife plainly [gave] the world implicit permission to access as many quotes as is *humanly* possible[,] a robot can collect more quotes than any human practicably could."[147] That is, Compulife had a reasonable expectation that others would not engage in massive, automated plagiarism.[148] Of course, Compulife could have taken more measures to keep its database secret; it could

---

[140] *Id.*

[141] *Data Economy: Radical transformation or dystopia?*, UNITED NATIONS (Jan. 2019), https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/FTQ_1_Jan_2019.pdf.

[142] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1296 (11th Cir. 2020).

[143] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f; *see also* JAGER, *supra* note 138, § 5:15.

[144] Trandes Corp. v. Guy F. Atkinson Co., 996 F.2d 655, 663–64, 663 n.8 (4th Cir. 1993); *see also* Samuel J. LaRoque, Note, *Reverse Engineering and Trade Secrets in the Post-*Alice *World*, 66 KANS. L. REV. 436, 438 (2017); Q-Co Indus., Inc. v. Hoffman, 625 F.Supp. 608, 617 (S.D.N.Y. 1985).

[145] *See* Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 372 (2017); JAGER, *supra* note 138, § 5:15 ("[S]ecrecy is a vague concept at best . . . .").

[146] 18 U.S.C. § 1839(6)(A); *see also* USTA § 1(4)(ii); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b; RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. g.

[147] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1314 (11th Cir. 2020) (emphasis added).

[148] *See* Lynda J. Oswald, *The Role of "Commercial Morality" in Trade Secret Doctrine*, 96 NOTRE DAME L. REV. 125, 164–70 (2020) (explaining how courts use trade secret law to enforce standards of business ethics).

have added technological access restrictions (enforceable using the CFAA) or contractual restrictions (enforceable using contract law) to prevent scraping.[149] Compulife also could have taken its database entirely off the Internet—after all, Compulife made substantial revenue from selling encrypted PC copies of its database.[150] However, trade secret law exists to prevent such overinvestments in secrecy.[151] Indeed, this is why trade secret law merely requires reasonable measures and relative secrecy as opposed to absolute secrecy.[152] It is unwise policy to incentivize websites to add burdensome restrictions on scraping or to take their databases offline. These perverse incentives would prevent all scraping, harmful as well as beneficial.[153]

3. The "Independent Economic Value" Requirement

Still, even with the theoretical distinction between the public-facing data and the secret database, not all databases will be trade secrets. A trade secret must "derive[] independent economic value . . . from not being generally known."[154] This requirement imposes an important limitation on the scope of *Compulife*.

To elucidate this "independent economic value" standard, courts have turned to several factors, including "the value of the information" to the plaintiff; "the amount of money or effort expended in developing the information"; and "the ease or difficulty with which one could probably acquire or duplicate the information."[155] For example, if a database merely parroted public, standardized insurance rate tables, that database would fail to meet this threshold "independent economic value" requirement. Compulife's database was a trade secret because it was the unique result of a "proprietary calculation technique," extremely valuable, and the product of significant labor.[156]

Interestingly, the "independent economic value" standard fully embraces a "sweat of the brow," Lockean labor theory, which copyright law flatly rejected.[157] The "independent economic value" requirement also parallels the "substantial investment" requirement for the EU *sui generis* database right, which is discussed *infra* Section VI.

---

[149] *See* discussion *supra* Sections II.B & II.C.

[150] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1296 (11th Cir. 2020).

[151] Lemley, *supra* note 23, at 332–37.

[152] *See id.* at 348–50.

[153] *See* Section IV.

[154] 18 U.S.C. § 1839(3)(B); USTA (1985) § 1(4)(i).

[155] Bernier v. Merrill Air Eng'rs, 770 A.2d 97, 107 (Me. 2001).

[156] Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808-JMH, 2018 WL 11033483, at *18 (S.D. Fla. Mar. 12, 2018).

[157] Ajaxo Inc. v. E*Trade Fin. Corp., 187 Cal. App. 4th 1295, 1311–1312 (2010) (Trade secret law protects the "right to have the ingenuity and industry one invests in the success of the business or occupation protected from the gratuitous use of that 'sweat-of-the-brow' by others."); Eric E. Johnson, *Trade Secret Subject Matter*, 33 HAMLINE L. REV. 545, 558 (2010).

D. Prong 2: Acquisition by "Improper Means"

1. The Eleventh Circuit's Decision

In *Compulife*, the district court found that scraping could not be misappropriation because "any member of the public can visit the website . . . to obtain a quote and there is no restriction on how an individual uses such a quote."[158] The Eleventh Circuit reversed, holding that scraping could be acquisition by improper means even when the scraping was performed on a publicly accessible website:

> [T]he fact that the defendants took the quotes from a publicly accessible site [does not] automatically mean that the taking was authorized or otherwise proper. Although Compulife has plainly given the world implicit permission to access as many quotes as is *humanly* possible, a robot can collect more quotes than any human practicably could. So, while manually accessing quotes from Compulife's database is unlikely ever to constitute improper means, using a bot to collect an otherwise infeasible amount of data may well be—in the same way that using aerial photography may be improper when a secret is exposed to view from above.[159]

Critics have attacked *Compulife*'s improper means analysis for creating an unclear, imprecise standard that dramatically expands scraping liability.[160] Admittedly, *Compulife* does interpret "improper means" broadly—but as Section III.C.2 explains, this is doctrinally sound because courts have broad discretion in improper means analysis. Moreover, as discussed in Section III.C.3, there are ways to judiciously limit scraping liability and curb *Compulife*'s ostensibly broad effects.

2. Improper Means Is a Broad Concept

The second prong of a trade secret claim is establishing that the acquisition of the trade secret was "improper." This standard is very malleable and subject to significant judicial discretion.[161] Certainly, illegal conduct (i.e., conduct that violates an independent legal norm), such as theft, bribery, and wiretapping, is

---

[158] *Compulife*, 2018 WL 11033483, at *19.

[159] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1314 (11th Cir. 2020) (emphasis in original) (citing E. I. du Pont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013 (5th Cir. 1970); Physicians Interactive v. Lathian Sys., Inc., No. CA 03-1193-A, 2003 WL 23018270, at *8 (E.D. Va. Dec. 5, 2003)).

[160] Peter J. Toren, *'Improper Means': The Eleventh Circuit's Very Dubious Trade Secrets Decision in Compulife Software v. Newman (Part II)*, IPWATCHDOG (July 14, 2020), https://www.ipwatchdog.com/2020/07/14/improper-means-eleventh-circuits-dubious-trade-secrets-decision-compulife-software-v-newman-part-ii/id=123265/; *see* McCarthy, *supra* note 134.

[161] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c ("It is not possible to formulate a comprehensive list of the conduct that constitutes 'improper' means.").

improper.[162] Contractual breaches and circumvention of technological access restrictions, which are also violations of independent legal norms, are also improper.[163] However, "[a]ctions may be 'improper' for trade-secret purposes even if not independently unlawful."[164] The landmark case for this proposition—and the case *Compulife* relied on—is the Fifth Circuit's decision in *E. I. du Pont deNemours & Co. v. Christopher*.[165]

In *Christopher*, the defendant took aerial photographs of the plaintiff's trade secret, an unfinished factory.[166] The defendants argued that because they had not violated an independent legal norm—that they "conducted all of their activities in public airspace, violated no government aviation standard, did not breach any confidential relation, and did not engage in any fraudulent or illegal conduct"—their actions were not "improper" under trade secret law.[167] However, even though the defendant's conduct did not violate an independent legal norm, it was improper and actionable under trade secret law.[168] The Fifth Circuit explained:

> We should not require a person or corporation to take unreasonable precautions to prevent another from doing that which he ought not do in the first place. Reasonable precautions against predatory eyes we may require, but an impenetrable fortress is an unreasonable requirement. . . . "Improper" will always be a word of many nuances, determined by time, place, and circumstances. We therefore need not proclaim a catalogue of commercial improprieties. Clearly, however, one of its commandments does say "thou shall not appropriate a trade secret through deviousness under circumstances in which countervailing defenses are not reasonably available."[169]

In *Christopher*, the plaintiff had taken reasonable precautions against theft and did not reasonably expect aerial espionage. Thus, "[t]o require [plaintiff] to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy's trick."[170]

---

[162] *See* 18 U.S.C. § 1839(6); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c.

[163] William E. Hilton, *What Sort of Improper Conduct Constitutes Misappropriation of a Trade Secret*, 30 IDEA J.L. & TECH. 287, 294–96 (1990); Robert G. Bone, *The Still (Shaky) Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1805 (2014); Physicians Interactive v. Lathian Sys., Inc., No. CA 03-1193-A, 2003 WL 23018270, at *8 (E.D. Va. Dec. 5, 2003) (finding computer hacking to be improper means).

[164] *See* Compulife Software Inc. v. Newman, 959 F.3d 1288, 1312 (11th Cir. 2020) (citing E. I. du Pont deNemours & Co. v. Christopher, 431 F.2d 1012, 1014 (5th Cir. 1970) (taking aerial photographs actionable as trade secret misappropriation)).

[165] E. I. du Pont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), *cert. denied*, 400 U.S. 1024 (1971).

[166] *Id.* at 1013.

[167] *Id.* at 1014.

[168] *Id.*

[169] *Id.* at 1017.

[170] *Id.* at 1016.

The *Compulife* court applied *Christopher* to hold that scraping could be improper, even if the scraping did not violate any separate legal norm such as contract law or the CFAA.[171] In *Christopher*, anyone could have lawfully flown over the plaintiff's factory.[172] However, when the defendant flew over the plaintiff's factory and took pictures for corporate espionage purposes, the defendant violated trade secret law.[173] Similarly, in *Compulife*, any human could freely visit the plaintiff's website.[174] But when the defendant used bots to scrape for purposes of creating an identical, competing product, the defendant misappropriated Compulife's valuable trade secrets.[175] Simply put, a "trade-secret owner's 'failure to place a usage restriction on its website' [does] not automatically render the hacking proper."[176]

Unfortunately, there is no clear-cut test for distinguishing between proper and improper means—between a lawful flyover and a trade secret misappropriating flyover—when no independent legal norm has been violated.[177] To this end, courts have typically rationalized the muddy proper-improper means distinction by looking at whether the defendant violated "standards of commercial morality."[178] These "standards of commercial morality" are themselves very ambiguous. In many instances, it amounts to nothing more than an application of an "I know it when I see it" test.[179] The defendant's scraping in *Compulife* tugs at our innate intuitions of unfair competition.[180] Something smelled rotten, and the Eleventh Circuit acted accordingly.[181]

In response to *Compulife*'s reliance on *Christopher*, critics attacked the precedential value of *Christopher*:

> While *Christopher* has become widely cited in textbooks, scholarly commentary and treaties, the *Compulife* decision is arguably the first appellate decision in more than 50 years that has relied upon

---

[171] *Compulife*, 959 F.3d at 1314 (citing *Christopher*, 431 F.2d at 1013).

[172] *Christopher*, 431 F.2d at 1014.

[173] *Id.*

[174] *Compulife*, 959 F.3d at 1314.

[175] *Id.* ("So, while manually accessing quotes from Compulife's database is unlikely ever to constitute improper means, using a bot to collect an otherwise infeasible amount of data may well be—in the same way that using aerial photography may be improper when a secret is exposed to view from above.").

[176] *Id.* at 1315 (quoting *Physicians Interactive v. Lathian Sys., Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *8 (E.D. Va. Dec. 5, 2003)).

[177] *See* Oswald, *supra* note 148, at 166–67.

[178] *Id.* (citing RESTATEMENT (FIRST) OF TORTS § 757 cmt. f.

[179] *Id.* at 168.

[180] *See* Section IV.C (explaining how the defendant was a free rider); *see also* Don Wiesner & Anita Cava, *Stealing Trade Secrets Ethically*, 47 MD. L. REV. 1076, 1104–1127 (1988) (describing "standards of commercial morality").

[181] *See* WILLIAM SHAKESPEARE, HAMLET, act 1, sc. 4, l. 65 ("Something is rotten in the state of Denmark.").

> *Christopher*, and which defendants were liable despite having broken no law and having breached no contract or confidential relationship. Surely, if other appellate decisions had involved similar circumstances to *Christopher*, the court in *Compulife* would have cited such a case.[182]

Such criticisms, however, are unavailing. The Supreme Court has approvingly cited *Christopher*.[183] Further, the lack of appellate reliance on *Christopher* is more reflective of the infrequent, cutting-edge situations *Christopher* is meant to address. Professor Lynda Oswald explains:

> *Christopher* provides an effective framework for analyzing cutting-edge misappropriation cases where black letter law may not provide an answer. Even if the competitive behavior at issue is not technically unlawful or in breach of contract, it nonetheless may give rise to liability if it is contrary to public policy imperatives of fair trade or below generally accepted commercial or societal norms.[184]

Ultimately, by decoupling *improper* means from *unlawful* means, *Christopher* and *Compulife* give courts significant discretion in ascribing trade secret misappropriation liability.[185] Under the broadest reading of *Christopher* and *Compulife*, any method of copying trade secrets can be improper means. That said, courts have typically constrained their analyses by looking at whether the defendant violated "standards of commercial morality."[186]

3. Guidance for Improper Means Analysis

Given that the commercial morality standard is vague and unhelpful,[187] this Section provides several guiding principles for courts to apply when analyzing improper means in the context of data scraping. First, the amount of data copied affects the analysis. Importantly, and correctly, the Eleventh Circuit did not hold that scraping is *per se* improper. Only scraping a substantial amount, such that "the block of data that the defendants took was large enough to constitute appropriation

---

[182] Toren, *supra* note 160.

[183] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475–76 (1974) ("The law also protects the holder of a trade secret against disclosure or use when the knowledge is gained, not by the owner's volition, but by some 'improper means,' which may include theft, wiretapping, or even aerial reconnaissance." (citing E. I. du Pont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970))).

[184] Lynda J. Oswald, *The 50th Anniversary of E.I. DuPont deNemours & Co. v. Christopher*, AIPLA, https://www.aipla.org/list/innovate-articles/the-50th-anniversary-of-e.i.-dupont-denemours-co.-v.-christopher (last visited Jan. 30, 2021).

[185] *See* James Pooley, *Gathering Business Data? Be Careful, Mom is Watching—A Comment on Data Scraping and the Compulife Case*, IPWATCHDOG (Sept. 20, 2020), https://www.ipwatchdog.com/2020/09/20/gathering-business-data-careful-mom-watching-comment-data-scraping-compulife-case/id=125377/ (arguing *Compulife* was rightly decided).

[186] *See Christopher*, 431 F.2d at 1016; *see also* Oswald, *supra* note 148, at 166.

[187] Oswald, *supra* note 148, at 166.

of the [d]atabase itself," is improper.[188] The substantial copying requirement allows courts to police the line between fair and unfair competition and between harmful free-riding and beneficial dissemination of information.

Another way to limit and guide judicial discretion under *Compulife* is to look to "principles of public policy."[189] In *Compulife*, the defendant used the scraped data to offer a directly competing, identical product. Had the *Compulife* defendant used the scraped data to perform scientific research on insurance rates, it would have been a different case.[190] Consider another hypothetical: what if plaintiff Compulife's website were the sole source for insurance rate data and Compulife sought to eliminate competition by preventing scraping? In this hypothetical, the plaintiff website would have a weaker argument that scraping was improper because of antitrust issues.[191] The caselaw on copyright fair use, unfair competition, and common law misappropriation ("hot news" tort) can provide "principles of public policy" to guide courts in deciding these difficult edge cases.

First, courts may draw from copyright law's fair use doctrine.[192] Even though trade secret law does not have a fair use defense,[193] given the flexibility of improper means analysis, courts should still look to fair use factors such as the "purpose and character of the [defendant's scraping], including whether . . . [it] is of a commercial nature or is for nonprofit educational purposes" and "the effect of the use upon the potential market for or value of the copyrighted work."[194] For example, in *Perfect 10 v. Amazon.com*, a magazine sued Google under copyright law for scraping thumbnail images of its magazine covers as part of Google Image Search.[195] The Ninth Circuit found Google's scraping to be copyright fair use because it was highly transformative—meaning Google's use was "fundamentally different from the use intended by" the plaintiff—and because it "provided a significant benefit to the public."[196]

Second, courts may draw from unfair competition law. For example, common law misappropriation doctrine emphasizes factors like whether "a defendant's use

---

[188] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1316 (11th Cir. 2020).

[189] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c. ("The propriety of the acquisition must be evaluated in light of all the circumstances of the case, including whether the means of acquisition are inconsistent with accepted principles of public policy . . . .").

[190] *See* Sandvig v. Barr, 451 F. Supp. 3d 73, (D.D.C. 2020)

[191] *See* Ioannis Drivas, Comment, *Liability for Data Scraping Prohibitions under the Refusal to Deal Doctrine*, 86 U. CHI. L. REV. 1901 (2019) (arguing that prohibiting scraping in such circumstances would violate antitrust law).

[192] *See* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007) (scraping was fair use); Kelly v. Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002) *withdrawn, re-filed at* 336 F.3d 811 (9th Cir. 2003) (same).

[193] *See generally* Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401 (2014).

[194] 17 U.S.C. § 107.

[195] *Perfect 10, Inc.*, 508 F.3d at 1155–56.

[196] *Id.* at 1168.

of the information constitutes free-riding on the plaintiff's efforts" and whether "the defendant is in direct competition with a product or service offered by the plaintiffs."[197] In *NBA v. Motorola*, Motorola and STATS created the SportsTrax paging system, which provided users with live statistics on basketball games.[198] STATS's employees would watch NBA games live, calculate game statistics, and input the statistics onto a computer, which then transmitted the data to Motorola's SportsTrax pagers.[199] In response to the NBA's "hot news" tort claim against SportsTrax, the Second Circuit found that the SportsTrax system was not competing with the NBA because the NBA's product was the game itself.[200] The Second Circuit further held that even if there were competition between SportsTrax and the NBA in the business of sports statistics, SportsTrax was not free-riding because SportsTrax expended its own effort to compile the sports statistics.[201]

Similarly, in *hiQ v. LinkedIn*, the Ninth Circuit granted a preliminary injunction enjoining LinkedIn's attempts to prevent hiQ's scraping because hiQ showed a sufficient likelihood of success on its argument that LinkedIn's scraping prohibition constituted an intentional interference with contract.[202] There, the court considered, and rejected, LinkedIn's defense that its conduct was a "legitimate business purpose" because:

> If companies like LinkedIn, whose servers hold vast amounts of public data, are permitted selectively to ban only potential competitors from accessing and using that otherwise public data, the result—complete exclusion of the original innovator in aggregating and analyzing the public information—may well be considered unfair competition under California law.[203]

The Ninth Circuit's analysis in *hiQ* recognized the anti-competitive dangers of "information monopolies"—of allowing dominant platforms to exercise monopolistic power over their data.[204] Given the value and utility of data, the power to exclude access to data is tantamount to the power to exclude entry into a market.[205]

---

[197] Nat'l Basketball Ass'n v. Motorola, 105 F.3d 841, 845 (2d Cir. 1997).

[198] *Id.* at 845.

[199] *Id.*

[200] *Id.* at 853.

[201] *See id.*

[202] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022).

[203] *Id.* at 1193–94.

[204] *Id.* at 1202 ("[G]iving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.").

[205] *See generally* Stucke, *supra* note 14.

Lastly, reverse engineering and independent creation are not improper means.[206] However, a data scraper's argument that it can reverse engineer the database using scraping is flawed. Reverse engineering is "starting with the known product and working backward to divine the process which aided in its development."[207] In the context of data scraping, the starting product is an individual piece of data. The database—with its attendant search functionalities and systematic organization—is not the starting point because it is secret and hidden behind the website. In other words, true reverse engineering does not utilize the comprehensive search functionalities and systematic organization of a website and its underlying database. Scraping is only feasible because the scraper takes advantage of such search functionalities and systematic organization. For example, in *Compulife*, the scraper was only able to scrape the data by inputting various combinations of data into the website. Without the search functionalities and systematic organization created by the website, data scrapers would not even be able to scrape.

In sum, this Section provided guideposts to courts applying *Compulife*. courts may draw from copyright fair use doctrine and unfair competition law to concretely define the "standards of commercial morality" and distinguish between beneficial and harmful scraping and between legitimate competition and free-riding and/or anti-competitive monopolization of data. Unfortunately, however, like much of trade secret law, these guideposts are vague standards rather than bright-line rules. More work needs to be done to delineate these standards and identify difficult edge cases. Still, as explained in Section V, these guideposts at least ask the right questions: the two main alternative causes of action—contract law and the CFAA—pin liability on the wrong factors.

E. Summary of the Compulife *Theory*

Sections III.C and III.D reconciled *Compulife* with existing trade secret law and fleshed out the substance of a trade secret cause of action. To summarize, the plaintiff may recover under the *Compulife* trade secret theory by showing: (1) the underlying database is a trade secret, meaning that (a) the database as a whole is not generally known to others, and (b) the database has independent economic value; and (2) scraping is improper, which involves consideration of whether (a) the defendant scraped a substantial portion, and (b) liability advances "principles of public policy," such as the values underlying the copyright fair use doctrine, unfair competition law, and antitrust principles. Table 1 below summarizes the data scraping legal landscape and how a trade secret theory interacts with the various other doctrines. The remainder of this Note discusses the policy implications of the *Compulife* theory.

---

[206] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 490 (1974) (announcing reverse engineering and independent creation to be absolute defenses); 18 U.S.C. § 1839(6)(B) (DTSA explicitly codifies these defenses).

[207] *Kewanee*, 416 U.S. at 476.

Table 1. Summary of the data scraping legal landscape.

	Contract	**CFAA**	**Copyright**	***Compulife* Trade Secret Theory**
Threshold requirement for protection of databases	Terms of service on website	Technological and/or contractual access restrictions on website	Database is original (some minimal degree of creativity)	Underlying database is secret and has independent economic value[§]
			Rejection of Lockean labor	Embraces Lockean labor
Protection of databases	Yes, regardless of the database's value	Yes, regardless of the database's value	"Thin" because most databases are not original	Yes, if database meets threshold requirements establishing value
Theory of liability	Existence of binding contract (notice of terms of service)	Criminal trespass (circumventing access restrictions)	Copying information and fair use defense	Copying information by improper means[‡]
Supported by IP policies (proper balance between website's interests and society's interests)[π]	No	No	Yes	Yes
Monetary Remedies	Actual damages	Actual damages	Actual damages, statutory damages, defendant's profits	Actual damages, unjust enrichment, reasonable royalties
Injunctive Relief	Rare	Yes	Yes	Yes
Source	State law	Federal law	Federal law	Federal and state law[*]

[§] *See* Section III.C.
[‡] *See* Section III.D.
[π] *See* Sections IV & V.
[*] Federal copyright law likely preempts a state law version of *Compulife*, but a federal law version of *Compulife* grounded in the DTSA survives un-preempted. *See* Section V.C.

IV. POLICY JUSTIFICATIONS FOR *COMPULIFE*

This Section describes the policy rationales for the *Compulife* trade secret theory. First, *Compulife*, like other intellectual property doctrines, simultaneously incentivizes the creation and disclosure of intellectual property. Second, *Compulife*'s independent economic value requirement draws upon a Lockean labor theory of property. Finally, *Compulife* supports equity and standards of commercial morality, allowing courts to draw lines between fair and unfair scraping practices.

A. Economic Rationale: Incentive to Create and Disclose

The fundamental rationale behind copyright and patent law is that these legal systems simultaneously incentivize the creation and disclosure of intellectual property.[208] This same rationale supports the *Compulife* trade secret theory.

First, by protecting databases, the *Compulife* theory incentivizes the creation of databases.[209] Like other information products, databases are public goods in that they are costly to create but easy to copy (i.e., free ride). Without an incentive to create, there would be an underinvestment in the production of databases. This incentivization is especially important because U.S. intellectual property law—unlike EU law—provides limited protection for and incentivization to create databases.[210] Still, the incentivization is not boundless. The "independent economic value" requirement filters out those databases undeserving of protection, just like patent law's novelty requirement and copyright's originality requirement do. For example, a simple multiplication database would have no independent economic value; though, of course, data scrapers would be unlikely to scrape a database with no independent economic value. Because *Compulife* has the threshold independent economic value requirement while quasi-IP doctrines do not, *Compulife* properly incentivizes websites to create value-adding databases.

Second, the *Compulife* trade secret theory—perhaps, paradoxically—incentivizes disclosure.[211] The key is that "the legal protection trade secret law provides serves as a *substitute* for investments in [] secrecy that companies might otherwise make."[212] In other words, trade secret law prevents an overinvestment in

---

[208] Lemley, *supra* note 23, at 329–41.

[209] *See id.* at 329–32; *see also* Harper & Row v. Nation Enterprises, 471 U.S. 539, 558 (1985) ("[I]t should not be forgotten that the Framers intended copyright itself to be the engine of free expression.").

[210] *See* discussion *supra* Section II.A (discussing thin copyright protection) & Section VI (discussing EU *sui generis* database right).

[211] *See* Lemley, *supra* note 23, at 331–37 ("Paradoxically, however, trade secret law actually encourages broader disclosure and use of information, not secrecy.").

[212] *Id.* at 333–34 (emphasis in original). Without trade secret law there would be a socially wasteful "arms race." Bone, *supra* note 163, at 1807–08. This "arms race" occurs "as the owner increases its investment in precautions, the appropriator increases its investment in stealing the secret, which then prompts the owner to increase precautions even further to counter the more serious threat, and so on." *Id.*

secrecy. Without *Compulife*, websites may turn to technological access restrictions (enforceable using the CFAA) and terms of service restrictions (enforceable using contract law) to protect their databases. Technological access and terms of service restrictions could "impose [] social cost[s] by restricting the flow of information."[213] These scraping-prevention mechanisms would prevent all scraping, beneficial and harmful. These restrictions can also be annoying to users. Slogging through CAPTCHAs and clickwrap terms of service make for an unpleasant Internet experience.

Compulife did not have technological access or terms of service restrictions on its website. Had the Eleventh Circuit held for the defendant, Compulife could have been incentivized to add these restrictions. Perhaps, Compulife would have required users to create a free account prior to using the generator. Or, even more extreme, Compulife could have taken its generator completely offline because Compulife generated substantial revenue by selling its database as a stand-alone PC version.[214] If we want an Internet that fosters the sharing of information, Compulife's decision to disclose and impose minimal restrictions should be incentivized, not discouraged.

B. Lockean Labor or "Sweat of the Brow" Theory

Under the Lockean labor conception of property, when "a person removes a resource from nature and applies labor to it, that resource would become that person's property."[215] Copyright law flatly rejected a Lockean labor theory in favor of an originality standard.[216] Meanwhile, trade secret law—through the independent economic value requirement—fully embraces the Lockean labor theory.[217] Websites have expended labor in creating databases, and under the Lockean labor theory, they should receive property rights in them.[218]

One rationale for the Lockean labor theory is utilitarian. Property rights incentivize websites to expend labor to create databases that add valuable

---

[213] Lemley, *supra* note 23, at 334.

[214] *See* Compulife Software Inc. v. Newman, 959 F.3d 1288, 1296–97 (11th Cir. 2020).

[215] Tabrez Y. Ebrahim, *Artificial Intelligence Inventions & Patent Disclosure*, 125 PENN ST. L. REV. 147, 201 (2020).

[216] Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991).

[217] One of the factors in assessing "independent economic value" is "the amount of money or effort expended in developing the information." Bernier v. Merrill Air Eng'rs, 770 A.2d 97, 107 (Me. 2001).

[218] *See* Eric R. Claeys, *Private Law Theory and Corrective Justice in Trade Secrecy*, 4 J. TORT L. 1, 33 (2011) ("[W]hen a claimant-competitor develops a minimally novel intellectual work, his discovery or information gathering constitutes intellectual labor . . . [, and therefore] deserves a reward for having contributed the discovery or assembly to society's store of knowledge."); *see also* Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1544–49 (1993) (presenting Lockean argument); Michael Risch, *Why Do We Have Trade Secrets?*, 11 INTELL. PROP. L. REV. 1, 28–33 (2007).

knowledge to society.[219] Without this incentive, websites would not expend labor to create databases.[220] Another rationale for the Lockean labor theory posits that websites deserve property rights in their databases because of the labor they expended.[221] In short, individuals own themselves, including the fruits of their labor, such as intellectual creations. However, both conceptions of the Lockean labor theory still require the database to have added some value to society. Under the utilitarian lens, society does not need to incentivize worthless databases.[222] Similarly, in the deserts-based rationale, the laborer does not deserve a property right for something that does not benefit society.[223]

The deserts-based conception of Lockean labor provides especially strong support for *Compulife*'s application of trade secret law to databases given the failure of alternative regimes.[224] That is, the only way to reward a website with a property right for expending labor in creating a database is through trade secret law.[225]

The independent economic value requirement of trade secret law incorporates the Lockean labor theory. In contrast, the quasi-IP doctrines (CFAA and contract law) do not have an underlying Lockean labor threshold. Quasi-IP doctrines protect databases regardless of whether the website expended sufficient labor. So long as there are technological access or contractual restrictions on the website, the plaintiff gains quasi-IP rights in its database. As such, quasi-IP doctrines do not properly incentivize websites to produce databases that benefit society.

C. Equity and Standards of Commercial Morality

Another rationale for trade secret law is "that it helps maintain 'standards of commercial morality.'"[226] Without trade secret law, piracy would be commonplace, and business would grind to a halt.[227] Courts apply the concept of "commercial morality" to mete out fairness and sanction unfair business practices.[228] However,

---

[219] *See* Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L.J. 287, 305–10 (1988).

[220] *See id.*

[221] *See* LAWRENCE BECKER, PROPERTY RIGHTS: PHILOSOPHIC FOUNDATIONS 48–56 (1977).

[222] *See* Hughes, *supra* note 219, at 305–10.

[223] *See* BECKER, *supra* note 221, at 55 ("[I]t should be noticed that the labor-desert argument does nothing to establish entitlement in cases where the laborer's efforts have not benefited anyone else. Deserving a benefit for producing something which only you profit from is a strange notion.").

[224] *See* discussion *supra* Section II.A (discussing copyright law's failure). Data is not patentable. *See* 35 U.S.C. § 101; Diamond v. Chakrabarty, 447 U.S. 303, 309 (1980) ("The laws of nature, physical phenomena, and abstract ideas have been held not patentable.").

[225] Of course, the CFAA and contract law give websites quasi-property rights. But for reasons explained *infra* Section V, IP law (i.e., trade secret law) is a better way to propertize the Internet.

[226] Varadarajan, *supra* note 145, at 370; *see also* JAGER, *supra* note 138, § 1:13; *cf.* Lemley, *supra* note 23, at 327–28 (critiquing theory).

[227] JAGER, *supra* note 138, § 1:13.

[228] Oswald, *supra* note 148, at 164–170.

the "standards of commercial morality" are extraordinarily vague.[229] In many instances, the standards amount to nothing more than an "I know it when I see it" test.[230] But in *Compulife*, the defendant clearly violated these standards of business ethics because the defendant's scraping—its wholesale copying to create an identical, competing product—was a textbook example of unfair free-riding.[231]

Trade secret law is fundamentally an equitable device that enforces fairness among business competitors.[232] These equitable considerations underlie *Compulife*. Compulife had no alternative legal remedies besides trade secret law—its CFAA, contract, and copyright law claims failed or would have failed.[233] As such, the *Compulife* court turned to the only available doctrine (trade secret law) to punish a patently unfair practice.[234] As demonstrated here, trade secret law, and the values underlying it, are uniquely suited to providing protection for valuable databases.

V. *COMPULIFE* FILLS THE DATABASE IP LAW GAP

This Section argues that trade secret law is a better conceptualization of the data scraping problem than the alternative quasi-IP doctrines because trade secret law, as a branch of IP law, ask the appropriate questions: How much data was taken? Was the database worthy of protection under trade secret law's "sweat of the brow" theory? What were the purposes of scraping? Meanwhile, CFAA liability depends on concepts of criminal trespass law, and contract law liability depends on the existence of a contract, which boils down to whether a scraper has notice of a website's terms of service. Further, courts can ground *Compulife* in the federal DTSA to create a uniform, national standard for data scraping.

Plaintiffs also have incentives to bring trade secret claims under *Compulife* because trade secret law has practical advantages. Trade secret law provides a broad suite of remedies (including injunctive relief, unjust enrichment, and reasonable royalties), and plaintiffs can assert federal subject matter jurisdiction using the DTSA.

---

[229] Wiesner & Cava, *supra* note 180 (concluding that courts do not apply "standards of commercial morality" consistently).

[230] Oswald, *supra* note 148, at 166.

[231] WIPO, PROTECTION AGAINST UNFAIR COMPETITION 55 (1994) (WIPO Pub. No. 725(E)) (Free riding is "any act that a competitor or another market participant undertakes with the intention of directly exploiting another person's industrial or commercial achievement for his own business purposes without substantially departing from the original achievement."); *see* Pooley, *supra* note 185 ("The foundation of it all, as the Supreme Court said, is the idea that business behavior should be ethical. And as we all know, ethics is highly contextual and situational . . . . I think that the court in the *Compulife* case got it right, because what the startup did seemed unfair and improper.").

[232] *See* Oswald, *supra* note 148, at 166–70 (discussing equitable power of trade secret law).

[233] *See* discussion *supra* Section II.

[234] Had Compulife not raised a trade secret claim it may have won on an unfair competition claim. The distinction between trade secret law and unfair competition law is murky as some characterize trade secret law as a flavor of unfair competition law. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45.

A. The Appeal of Using Trade Secret Law to Fill the Database Gap

Instead of using quasi-IP doctrines, we can use trade secret law to fill the database IP law gap left by copyright.[235] The *Compulife* theory described in Section III.E asks the right questions in data scraping cases. Instead of deciding liability based on analogies to physical trespass law or on the existence of a contract, courts can consider IP law norms designed to balance database protection with interests in competition and disseminating information. The CFAA and contract law are also unhinged from an underlying intellectual property rationale such as an economic theory or a Lockean labor theory.

Using trade secret law, courts can look at how much data was copied.[236] The substantial copying standard ensures that those users who merely consult the database a few times are not subject to liability.[237] Contract law and the CFAA do not have this limitation. Next, the improper means analysis factors discussed in Section III.D.3—specifically, the fair use factors—allow courts to distinguish between patently unfair free-riding like that in *Compulife* and socially beneficial scraping, such as scraping for scientific research purposes. Neither the CFAA nor contract law has a fair use mechanism.[238] Trade secret law also does not have a fair use doctrine, but courts may incorporate a fair use analysis into its improper means analysis.[239] In close cases like those involving price aggregators (websites that scrape prices from online shopping websites), courts can also look at unfair competition factors like whether scraping promotes competition or whether the scraper impermissibly free rides.[240] By no means will the analysis be simple, but at least courts will be attuned to the relevant factors. Using these factors, courts can find the balance between the website's interests in exploiting its database and society's and scraper's interests in competition and free speech.

Using *Compulife*, courts can also ask the threshold question of whether the data warrants protection as a trade secret—whether the database has become generally

---

[235] This Note treats trade secret law as IP law, but there is actually significant scholarly debate over how to characterize trade secret law. *See, e.g.*, Lemley, *supra* note 23 (arguing trade secret law is IP law); Miguel Deutch, *The Property Concept of Trade Secrets in Anglo-American Law: An Ongoing Debate*, 31 U. RICH. L. REV. 313 (1997) (arguing trade secret law is property law); Thornton Robison, *The Confidence Game: An Approach to the Law About Trade Secrets*, 25 ARIZ. L. REV. 347, 383 (1983) (arguing trade secret law is contract law); Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241 (1998) (arguing trade secret law has no rational justification).

[236] *See* discussion *supra* Section III.D.3.

[237] *See id*.

[238] *See* Carrero, *supra* note 12, at 132 (arguing for a fair use-like exception to the CFAA); Ginsburg, *supra* note 35, at 165–71 (discussing whether contract law could have a fair use exception).

[239] *See* discussion *supra* Section III.D.3.

[240] *See, e.g.*, QVC, Inc. v. Resultly, LLC, 99 F. Supp. 3d 525 (E.D. Pa. 2015) (price aggregator case applying the CFAA).

known and whether the database has independent economic value.[241] This threshold question reinforces the economic and Lockean labor theories underlying trade secret law.[242] The *Compulife* theory will only grant intellectual property rights in and incentivize the creation of those databases that add value to society.[243] In contrast, the CFAA and contract law allow websites to transform databases otherwise undeserving of protection under trade secret law into intellectual property. To the CFAA and contract law, scraping from a database that took thousands of hours to create is the same as scraping from a database that took no effort to create. As such, the CFAA and contract law fail to incentivize the creation of value-adding databases. Furthermore, because *Compulife* asks these threshold questions, *Compulife* ensures that at least some databases will remain in the public domain, promoting free speech interests.

Moreover, as explained in Section IV.A, CFAA and contract law claims require websites to place technological access and contractual restrictions on their databases. Thus, the CFAA and contract law perversely incentivize websites to restrict the free flow of information. These restrictions—for example, CAPTCHAs and clickwrap terms of service—can also be annoying to users. However, the CFAA and contract law have one advantage over trade secret law in that technological access and contractual restrictions function to provide notice that scraping is unlawful.[244] Nevertheless, trade secret law has a scienter requirement that serves a similar notice function. If the scraper does not know or have reason to know that the database is a trade secret or that scraping is improper, the scraper has a defense.[245]

Additionally, contract law and CFAA damages are purely compensatory, which means the plaintiff can only recover for its actual loss.[246] To properly disincentivize copying, damages need to reflect the defendant's gain.[247] Otherwise, the defendant can simply continue infringing and write off the damages payout as a cost of doing business, in which case the plaintiff is insufficiently protected and inadequately

---

[241] *See* discussion *supra* Section III.C.3.

[242] *See* discussion *supra* Section IV.

[243] *See id.*

[244] "[U]sers have an interest in fair notice of the conditions of access." Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2192 (2004); *see also id.* at 2252–72 (analyzing the importance of notice).

[245] 18 U.S.C. § 1839(5)(A) ("'[M]isappropriation' means acquisition of a trade secret of another by a person who *knows or has reason to know* that the trade secret was acquired by improper means.") (emphasis added); *see* Lemley, *supra* note 23, at 349 n.164 (discussing scienter requirement); Lamb-Weston, Inc. v. McCain Foods, Ltd., 941 F.2d 970 (9th Cir. 1991) (same).

[246] *See* Sw. Airlines Co. v. BoardFirst, L.L.C., No. 3:06-CV-0891-B, 2007 WL 4823761, at *9–12 (N.D. Tex. Sept. 12, 2007) (analyzing contract damages in scraping claim); *see also* 18 U.S.C. § 1030(g) (CFAA damages are limited to compensatory damages.).

[247] Roger D. Blair and Thomas F. Cotter, *An Economic Analysis of Damages Rules in Intellectual Property Law*, 39 WM. & MARY L. REV. 1585, 1590 (1998) (arguing that the IP damages should "render[] the infringer no better off as a result of the infringement").

incentivized to create databases.[248] IP law recognizes the importance of damages in regulating the defendant's behavior: copyright, patent, trademark, and trade secret law all allow the plaintiff to recover beyond its actual loss, allowing the court to consider alternative damages methods such as unjust enrichment and reasonable royalties.[249]

Courts can also use trade secret law to create national, uniform standards for data scraping. While *Compulife* specifically applied the Florida Uniform Trade Secrets Act ("FUTSA"), the Eleventh Circuit assumed the FUTSA was identical to the federal DTSA.[250] Therefore, courts can apply *Compulife* using the DTSA to create national standards for data scraping. Indeed, one of Congress's goals in enacting the DTSA was to create "a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved."[251] In contrast, contract law and state unfair competition law claims are state law. Because websites transcend borders, uniformity is important. It would be nonsensical for a scraper in one state to get off scot-free but a scraper in another state to be liable.

Lastly, trade secret law preempts state unfair competition law.[252] As such, trade secret law can channel data scraping cases away from state law claims like the "hot news" tort, unjust enrichment, conversion, and trespass to chattel. Channeling is beneficial because it eliminates doctrinal overlap, allowing courts to use a single doctrinal tool to create a clear standard for data scraping liability.[253] However, trade secret law does not preempt contract law or the CFAA.[254] Thus, trade secret law cannot channel data scraping claims away from contract law or the CFAA. As such, many of the benefits of trade secret law may be unrealized in practice if websites

---

[248] *See id.*

[249] *See id.*; 17 U.S.C. § 504(a)(1) (copyright law); 35 U.S.C. § 284 (patent law); 15 U.S.C. § 1117(a)(1) (trademark law); 18 U.S.C. § 1836(b)(3)(B)(i)(II) (trade secret law).

[250] *See supra* note 128 and accompanying text.

[251] H.R. REP NO. 114-529, at 6 (2016); *see* S. REP. NO. 114-220, at 14–15 (2016).

[252] USTA § 7(a) (The Uniform Trade Secrets Act "displaces conflicting tort, restitutionary, and other law of this State providing civil remedies for misappropriation of a trade secret."); 18 U.S.C. § 1838; Richard F. Dole Jr., *Preemption of Other State Law by the Uniform Trade Secrets Act*, 17 SMU SCI. & TECH. L. REV. 95, 106–16 (2014) (explaining judicial interpretations of UTSA § 7(a)). To the extent a website concedes that the database is not a trade secret, there is a split on whether the unfair competition claims survive un-preempted. *See* Dole, *supra* note 252, at 106–16 (describing majority and minority views—the majority view is that the unfair competition claims are preempted).

[253] *See* Laura A. Heymann, *Overlapping Intellectual Property Doctrines: Election of Rights Versus Selection of Remedies*, 17 STAN. TECH. L. REV. 239 (2013) (discussing ways to regulate overlapping IP doctrines).

[254] *See* USTA § 7(b)(1) (UTSA does not preempt contract law); 18 U.S.C. § 1838 (DTSA does not preempt CFAA).

rely on trade secret law in conjunction with the CFAA and contract law.[255] This issue of doctrinal overlap is left for another day.[256]

B. The Appeal of Trade Secret Law for Plaintiffs

Trade secret law is also an attractive theory for plaintiff websites because it offers a broad suite of remedies, including injunctive relief, unjust enrichment, and reasonable royalties.[257] The CFAA occasionally allows for injunctive relief, and contract law, only in extraordinary circumstances, allows for injunctive relief.[258] Meanwhile, trade secret law routinely rewards injunctive relief because of the importance of protecting the trade secret—the database—from being generally known by others.[259]

Monetary damages under the CFAA and contract law are also limited. The default remedy in contract cases is actual (i.e., compensatory) damages.[260] Compensatory damages can be hard to show, especially when the data scraper uses the data for a different purpose than does the website.[261] Similarly, monetary damages for CFAA violations are "compensatory damages," which "are limited to economic damages."[262] Damages under the CFAA are also restricted to losses that are "incurred because of interruption of service."[263] CFAA plaintiffs cannot claim

---

[255] For example, trade secret law does not require the website to place contractual and/or technological access restrictions on the database. But a website may continue to use such restrictions so it can take advantage of contract law and the CFAA. In that case, trade secret law does not incentivize disclosure.

[256] *See* Heymann, *supra* note 253, at 242–275 (discussing ways to regulate overlapping IP doctrines). One of Professor Heymann's proposals is selection of remedies. Under this framework, if a plaintiff wants to recover trade secret specific remedies like unjust enrichment, the plaintiff can only assert trade secret claims. *Id.*

[257] JAGER, *supra* note 138, Ch. 7; RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 44–45; 18 U.S.C. 1836(3).

[258] 18 U.S.C. § 1030(g); Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004) ("[S]pecific relief is not the conventional remedy for breach of contract.").

[259] *See* Richard F. Dole, *Permanent Injunctive Relief for Trade Secret Misappropriation Without an Express Limit Upon Its Duration: The Uniform Trade Secrets Act Reconsidered*, 17 B.U. J. SCI. & TECH. L. 173 (2011).

[260] *Register.com*, 356 F.3d at 426 ("[T]he classic remedy for breach of contract is an action at law for monetary damages. If the injury complained of can be compensated by an award of monetary damages, then an adequate remedy at law exists and no irreparable injury may be found as a matter of law.").

[261] *See* Sw. Airlines Co. v. BoardFirst, L.L.C., No. 3:06-CV-0891-B, 2007 WL 4823761, at *9–12 (N.D. Tex. Sept. 12, 2007); Int'l Council of Shopping Centers, Inc. v. Info Quarter, LLC, No. 17-CV-5526 (AJN), 2019 WL 2004029, at *4 (S.D.N.Y. May 7, 2019) (dismissing contract claim for failure to specify damages).

[262] 18 U.S.C. § 1030(g).

[263] 18 U.S.C. § 1030(e)(11).

lost revenue if the scraping does not cause the website to go offline.[264] In contrast, trade secret law provides reasonable royalties and unjust enrichment damages, which can give plaintiffs much greater recovery.[265]

Lastly, plaintiffs can use the DTSA to assert federal subject matter jurisdiction. Contract law is state law, so it cannot provide subject matter jurisdiction. The CFAA is federal law, but to assert a CFAA violation, the plaintiff must show at least $5,000 of loss.[266] While $5,000 appears to be a low threshold, plaintiffs have, at times, failed to clear it.[267] In contrast, trade secret law has a very permissive standing threshold. So long as the trade secret is "related to a product or service used in, or intended for use in, interstate or foreign commerce," a plaintiff can assert a DTSA claim.[268] The very fact that the trade secret database is accessible on the Internet may satisfy the DTSA's interstate commerce requirement.[269]

C. Does Federal Copyright Law Preempt Compulife*?*

Compulife fills the database IP law gap left by copyright law, but does copyright law preempt the *Compulife* doctrine?[270] To the extent that *Compulife* is a state law

---

[264] *See* Nexans Wires S.A. v. Sark-USA, Inc., 166 F. App'x 559, 563–64 (2d Cir. 2006) ("Because it is undisputed that no interruption of service occurred in this case, [plaintiff's] asserted loss of $10 million is not a cognizable loss under the CFAA.").

[265] JAGER, *supra* note 138, Ch. 7.

[266] 18 U.S.C. § 1030(c)(4)(i)(I).

[267] *See, e.g.*, *Nexans Wires*, 166 F. App'x at 562–64.

[268] 18 U.S.C. § 1836(b).

[269] *See* Valeria G. Luster, *Let's Reinvent the Wheel: The Internet as a Means of Interstate Commerce in* United States v. Kieffer, 67 OKLA. L. REV. 589 (2015) (analyzing the Internet and Congress's Commerce Clause powers).

[270] There is also an interesting question of whether *Compulife* is constitutional under the Copyright Clause. Originality is a constitutional requirement of the Copyright Clause. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 346 (1991). Time-limited protection is also a constitutional requirement of the Copyright Clause. U.S. Const., art. I, § 8, cl. 8 ("The Congress shall have Power . . . To promote the Progress of Science and useful Arts, by securing for *limited Times* to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.") (emphasis added); Eldred v. Ashcroft, 537 U.S. 186 (2003) (analyzing the "limited Times" limitation). Trade secret law protects non-original databases, and trade secret protection can last indefinitely long. As such, the *Compulife* trade secret theory is at odds with the Copyright Clause. However, federal trade secret law is grounded in the Commerce Clause. *See* Conor Tucker, *The DTSA's Federalism Problem: Federal Court Jurisdiction over Trade Secrets*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1 (2017).

The constitutional question is whether indefinite trade secret protection of non-original databases unconstitutionally uses the Commerce Clause to make an end-around the time length and originality limitations of the Copyright Clause. This issue is unsettled. *See* Kiss Catalog, Ltd. v. Passport Int'l Prods., Inc., 405 F. Supp. 2d 1169, 1175 (C.D. Cal. 2005) (End-around is allowed: "once the Court concludes that the Statute does not fall within the purview of the Copyright Clause, it need no longer consider whether it complies with the limitations of the Copyright Clause."); United States v. Martignon, 346 F. Supp. 2d 413, 420 (S.D.N.Y. 2004), *vacated and remanded*, 492 F.3d 140 (2d Cir. 2007) (District court found that end-around was not allowed, holding that "copyright-like" statute was subject to Copyright Clause limitations. Second Circuit reversed.);

trade secret doctrine, *Compulife* is preempted by federal copyright law because the *Compulife* theory described in Section III.E is nearly indistinguishable from copyright liability.[271] However, *Compulife* can survive preemption challenges by being grounded in the federal DTSA.

Federal copyright law preempts state laws that (1) "come within the subject matter of copyright" and (2) provide rights that are "equivalent to any of the exclusive rights within the general scope of copyright."[272] For the first prong, "[a]s long as a work fits within one of the general subject matter categories (of federal statutory copyrights), [copyright] prevents the states from protecting it even if it fails to achieve federal statutory copyright because it is . . . lacking in originality to qualify."[273] Therefore, even if they do not get copyright protection, databases fall within copyright's subject matter as both "literary works" and "compilations."[274] To evaluate the second prong, courts apply the "extra element" test, which asks whether "one or more qualitatively different elements are required to constitute the state-created cause of action being asserted."[275] State trade secret laws typically escape preemption because acquisition by improper means is an "extra element."[276] However, improper means typically involve conduct that is independently wrongful, such as breach of a confidential relationship. The improper means in *Compulife* are much closer to plain old copying, which is already covered by

---

United States v. Moghadam, 175 F.3d 1269 (11th Cir. 1999) (There are "circumstances . . . in which the Commerce Clause cannot be used by Congress to eradicate a limitation upon Congress in another grant of power." However, the court ultimately held that the end-around was constitutional.); *see also* Galbraith, *supra* note 37, at 358–361 ("Congress cannot bypass the restrictions of the Intellectual Property Clause by enacting legislation to protect works that lack originality under a separate provision of the Constitution, such as the Commerce Clause.").

[271] *See* Citizens Info. Assocs., LLC v. Justmugshots.com, No. 1-12-CV-573-LY, 2013 WL 12076563, at *3 (W.D. Tex. Feb. 26, 2013) (In data scraping case, trade secret claim preempted by federal copyright law.).

[272] 17 U.S.C. § 301(b)(1) & (3); Crow v. Wainwright, 720 F.2d 1224, 1225–26 (11th Cir. 1983), *cert. denied*, 469 U.S. 819 (1984).

[273] H.R. REP. NO. 1476, 94th Cong., 2d Sess. 51, 131 (1976); *see* Harper & Row v. Nation Enters., 723 F.2d 195, 200 (2d Cir. 1983) ("The fact that portions of the Ford memoirs may consist of uncopyrightable material . . . does not take the work as a whole outside the subject matter protected by the Act."), *rev'd on other grounds*, 471 U.S. 539 (1985); Ultraflo Corp. v. Pelican Tank Parts, Inc., 845 F.3d 652, 656 (5th Cir. 2017) (Federal copyright law "preempts state protection of works that fall within the subject matter (that is, the scope) of copyright, regardless whether the works are actually afforded protection under the Copyright Act.").

[274] 17 U.S.C. § 102(a)(1) ("literary works" which are works "expressed in words, numbers, or other verbal or numerical symbols or indicia"); 17 U.S.C. § 103 (compilations).

[275] *Ultraflo*, 845 F.3d at 657 (quoting Alcatel USA, Inc. v. DGI Techs., Inc., 166 F.3d 772, 787 (5th Cir. 1999)).

[276] *See* GlobeRanger Corp. v. Software AG United States of Am., Inc., 836 F.3d 477, 488–91 (5th Cir. 2016) (Trade secret misappropriation involving breach of confidential relationship not preempted.).

copyright law.[277] Therefore, federal copyright law should preempt *Compulife* to the extent *Compulife* is state law.

But *Compulife* survives preemption challenges by being grounded in the federal DTSA. The *Compulife* court, like many other courts, assumed state and federal trade secret law were identical.[278] Therefore, the DTSA can be a vehicle for applying *Compulife* because the Copyright Act does not preempt other federal laws such as the DTSA.[279]

VI. THE EU *SUI GENERIS* DATABASE RIGHT

Unlike U.S. law, EU law has considered the data scraping problem using IP law, namely the *sui generis* database right. This Section argues that the *Compulife* trade secret theory emulates many aspects of the EU *sui generis* database right and is effectively the U.S. version of the EU *sui generis* database right. The EU *sui generis* database right shows that an IP law framework for data scraping can successfully function. Further, the U.S.'s adoption of the *Compulife* theory may draw upon the model of the EU *sui generis* database right, harmonizing U.S. law with international norms.

A. The EU Sui Generis *Database Right Fills the Database Gap*

EU copyright law is similar to U.S. copyright law in the "thin" protection it extends to databases.[280] Recognizing copyright law's failure to protect databases and the important role of databases "in the development of an information market," the EU created a *sui generis* database right in 1996.[281] This *sui generis* database right grants database creators an exclusive property right in the contents of their databases (i.e., the data).[282]

---

[277] *See Ultraflo*, 845 F.3d at 657–59 (Plaintiff asserted unfair competition by misappropriation claim and argued that "sweat of the brow" was an extra element allowing the claim to escape copyright preemption. The court rejected this claim and held that the misappropriation claim was preempted.); 17 U.S.C. § 106(1) (Copyright grants the exclusive right "to reproduce the copyrighted work in copies.").

[278] *See supra* note 128 and accompanying text.

[279] 17 U.S.C. § 301(d) ("Nothing in this title annuls or limits any rights or remedies under any other Federal statute.").

[280] *See* ESTELLE DERCLAYE, THE LEGAL PROTECTION OF DATABASES: A COMPARATIVE ANALYSIS 308–18 (2008) (discussing EU copyright law).

[281] *Id.* at 320 ("[T]he main investment in a database is in its contents. However, copyright does not protect the contents but only the database's structure. So taking the contents without the structure would not infringe. An additional protection was necessary to protect the contents."); Database Directive, recitals (7)–(12).

[282] The EU adopted a property right model, expressly rejecting an unfair competition model, which would "focus[] on the nature of conduct prohibited rather than providing ownership rights in particular subject matter." U.S. COPYRIGHT OFFICE, REPORT ON LEGAL PROTECTION FOR DATABASES 89 (1997), *available at* https://www.copyright.gov/reports/db4.pdf. "The [European] Commission has given several reasons for its change in approach [rejection of an unfair competition

Instead of relying on an originality requirement, the EU *sui generis* database right adopts a "sweat of the brow" theory.[283] The database right grants creators property rights to the contents of databases so long as "there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents."[284] EU cases analyzing the substantial investment requirement have drawn the line between protectable and non-protectable databases.[285]

The EU *sui generis* database right exists concurrently with and independently of whatever "thin" copyright rights that may exist in the database.[286] If a database meets the "substantial investment" requirement, the database maker is protected against the "extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."[287] This protection lasts for 15 years, but the term may be extended when there is a "substantial change . . . to the contents" and this substantial change itself satisfies the "substantial investment" requirement.[288]

Data scraping cases in the EU have been litigated under this database right.[289] For example, in *Innoweb BV v. Wegener ICT Media BV*, plaintiff Wegener operated a website hosting a database of used cars for sale.[290] The defendant Innoweb operated a "meta search engine," which searched through other databases not owned or operated by Innoweb in response to a user query.[291] Innoweb's meta search engine used Wegener's own search engine to search through Wegener's database and presented those results as Innoweb's own.[292] Ultimately, the Court of Justice of the European Union found Innoweb's scraping to be an infringing re-utilization of Wegener's database.[293] The CJEU described Innoweb's meta search

---

model], primarily: (1) the lack of established unfair competition laws in every country; (2) the need for producers to know what they own ahead of time, rather than waiting until someone engages in a use which a court finds wrongful; and (3) the commercial transferability of property rights." *Id.* at 90.

[283] Philip J. Cardinale, *Sui Generis Database Protection: Second Thoughts in the European Union and What It Means for the United States*, 6 CHI.-KENT J. INTELL. PROP. 157, 157–68 (2007).

[284] Database Directive, art. 7(1).

[285] *See, e.g.*, Case C-203/02, The British Horseracing Board Ltd v. William Hill Organization Ltd, 2004 E.C.R. I-333.

[286] *See* Database Directive, recitals (39), (45), (57), (58).

[287] Database Directive, art. 7(1).

[288] Database Directive, art. 10.

[289] *See, e.g.*, Case C-202/12, Innoweb BV v. Wegener ICT Media BV, 2013 E.C.R. I-850.

[290] *Id.* ¶ 8.

[291] *Id.* ¶ 9 ("A 'meta search engine' uses search engines from other websites, transferring queries from its users to those other search engines—a feature which differentiates meta search engines from general search engines such as Google.").

[292] *Id.*

[293] *Id.* ¶ 54 (The court assumed that Wegener's database met the substantial investment requirement. *Id.* ¶ 16.).

engine as a "parasitical competing product." [294] The CJEU explained how the defendant's scraping would cause the plaintiff website to lose revenue,[295] thereby disserving the *sui generis* database right's purpose in allowing the website to reap the rewards of its intellectual labor.[296]

B. Compulife *Emulates the EU* Sui Generis *Database Right*

Several legislative attempts have been made to enact a *sui generis* database right in the U.S., but these attempts have all failed.[297] The *Compulife* theory, however, effectively takes the place of a *sui generis* database right as it closely tracks the EU *sui generis* database right.

Both the *Compulife* trade secret theory and the EU *sui generis* database right are property rights, allowing for easy transfer and licensing.[298] *Compulife*'s independent economic value requirement parallels the *sui generis* database right's substantial investment requirement: both requirements are grounded in a Lockean labor "sweat of the brow" rationale, which copyright law rejected. Moreover, uniformity goals drive both *Compulife* and the *sui generis* database right. Courts adopting *Compulife* can use the DTSA to establish national, uniform standards on data scraping.[299] Similarly, the *sui generis* database right was intended to "harmonize[]" database protection across the EU.[300] Uniform rules for data scraping are necessary because cyberspace transcends jurisdictional borders.[301]

Compulife and the *sui generis* database right also approach the infringement analysis similarly. The *sui generis* database right applies to substantial scraping and would not apply to mere consultations.[302] Still, under the *sui generis* database right,

---

[294] *Id.* ¶ 48.

[295] *Id.* ¶ 41 ("That activity on the part of the operator of a dedicated meta search engine such as that at issue in the main proceedings creates a risk that the database maker will lose income, in particular the income from advertising on his website, thereby depriving that maker of revenue which should have enabled him to redeem the cost of the investment in setting up and operating the database.").

[296] *Id.* ¶ 36 ("To that end, the protection offered by the sui generis right under Directive 96/9 [Database Directive] is intended to ensure that the person who has taken the initiative and assumed the risk of making a substantial investment in terms of human, technical and/or financial resources in the setting up and operation of a database receives a return on his investment by protecting him against the unauthorized appropriation of the results of that investment.").

[297] Daniel J. Gervais, *The Protection of Databases*, 82 CHI.-KENT. L. REV. 1109, 1139–43 (2007).

[298] DERCLAYE, *supra* note 280, at 320.

[299] *See supra* note 128 and accompanying text.

[300] Database Directive, recitals (2) & (4).

[301] *See* Database Directive, recital (4).

[302] Database Directive, art. 8(1) ("The maker of a database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilizing insubstantial parts of its contents . . . ."); Case C-202/12, Innoweb BV v. Wegener ICT Media BV, 2013 E.C.R. I-850, ¶ 46 ("[T]he protection under Article 7 of Directive 96/9 does not cover consultation of a database.").

there is room for judicial discretion as "[t]he repeated and systematic extraction and/or re-utilization of *insubstantial* parts . . . implying acts . . . which unreasonably prejudice the legitimate interests of the maker of the database shall not be permitted."[303] Further, to constitute infringement under the *sui generis* database right, the extraction and/or re-utilization must "cause[] significant detriment, evaluated qualitatively or quantitatively, to the investment" of the database creator.[304] To this end, EU courts are instructed to:

> strike a fair balance between, on the one hand, the legitimate interest of the makers of databases in being able to redeem their substantial investment and, on the other hand, that of users and competitors of those makers in having access to the information contained in those databases and the possibility of creating innovative products based on that information.[305]

Likewise, the *Compulife* theory is limited to where the scraper has copied a substantial amount of data, but courts have broad discretion in improper means analysis to consider the effects of scraping on fair competition.[306] Both EU and U.S. courts are attuned to the need to balance proprietary rights with fair competition.

Finally, both the *Compulife* theory and the *sui generis* database right stop short of granting the database owner an ironclad exclusionary right as both allow defendants to raise independent creation and reverse engineering defenses.[307] However, the *sui generis* database right does not have a fair use defense, a deficiency that has been criticized.[308]

Despite the many similarities, the *Compulife* theory departs from the *sui generis* database right in one significant way. While the *sui generis* database right is time-limited to 15 years, trade secret law is not: a trade secret lasts as long as it satisfies the trade secret definition, which can be infinitely long. Infinite protection may present anti-competition issues, particularly in light of the fact that IP law's monopolistic grant is typically time-limited.[309] Moreover, indefinite protection may be unconstitutional.[310]

This is not fatal to *Compulife* for several reasons. First, even in the absence of *Compulife*, database owners can use the CFAA and contract law to protect their databases for indefinitely long time periods. In that sense, the doctrinal shift from

---

[303] Database Directive, art. 7(5) (emphasis added).

[304] Case C-762/19, CV-Online Latvia SIA v. Melons SIA, 2021 E.C.R. I-289, ¶ 39.

[305] *Id.* ¶ 41.

[306] *See* discussion *supra* Section III.D.

[307] *See* Database Directive, art. 7(2).

[308] *See* Matthias Leistner, *Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform*, 13–14 (Sept. 7, 2018), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3245937.

[309] *See* Drivas, *supra* note 191.

[310] *See supra* note 270 (discussing the constitutional issue of whether trade secret law and Commerce Clause can make end-around limitations of the Copyright Clause).

CFAA and contract law to *Compulife* does not change the status quo.[311] If anything, because a database loses its trade secret status once it becomes generally known, protection under trade secret law is practically shorter than that under the CFAA and contract law.[312] Second, when compared to U.S. copyright law, which can last as long as 120 years, the possibly indefinite protection for trade secrets appears less problematic. Lastly, the *sui generis* database right allows the term to be extended when there is a "substantial change . . . to the contents."[313] That is, the *sui generis* database right also allows database owners to obtain indefinite protection. Given that many databases are temporally dynamic and constantly updated, the EU *sui generis* database right is as broad-sweeping as *Compulife*. And, at any rate, trade secret law finds solid Constitutional grounding in the Commerce Clause, which does not contain any time-limited restrictions on proprietary rights.[314]

The *Compulife* theory parallels many aspects of the EU *sui generis* database right, thereby harmonizing U.S. law with international standards and creating more cohesive international IP norms. For example, the EU database directive has a reciprocity provision, meaning that non-EU nationals may receive protection under the *sui generis* database right only if their country provides "comparable protection to databases."[315] The adoption of *Compulife* in the U.S. will create a comparable database regime, allowing U.S.-origin databases to receive protection under the EU database directive.

Overall, the *sui generis* database right and *Compulife* both arose to address the same problem—the database void left by copyright law. Indeed, in light of all the similarities, *Compulife*'s trade secret theory is arguably the U.S.'s attempt to fashion its own *sui generis* database right. While legislators have failed to enact a *sui generis* database right, courts can use *Compulife* to develop trade secret law to mirror the EU *sui generis* database right. The success of the EU *sui generis* database right serves as an illuminating path forward for courts to apply *Compulife*.

VII. CONCLUSION

Before *Compulife*, criminal trespass law (i.e., the CFAA) and contract law were the battlegrounds for data scraping. These quasi-IP doctrines filled the gap left by copyright's "thin" protection of databases. This Note argues that the CFAA and contract law have been ineffective ways to consider the data scraping problem and that trade secret law is the better doctrinal framework.

On the surface, it appears that *Compulife* has turned trade secret law inside out by abandoning the concept of secrecy. This Note argues that *Compulife* is

---

[311] Duan, *supra* note 75, at 24 ("[T]here is no time limit on a CFAA-backed ad hoc 'copyright' regime.").

[312] The CFAA and contract law have no time restrictions.

[313] Database Directive, art. 10.

[314] *See supra* note 270 (discussing the constitutional issue of whether trade secret law and Commerce Clause can make end-around limitations of the Copyright Clause).

[315] Database Directive, recital (56), art. 11; *see* Gervais, *supra* note 297, at 1147.

reconcilable with existing trade secret jurisprudence because the analytical distinction is between public data and the secret database. While the elements set out for the trade secret cause of action are far from bright-line rules and trade secret law uses many ambiguous standards, this Note draws from existing trade secret jurisprudence to detail what the substance of these standards might look like for data scraping. Certainly, further judicial analysis is required to determine the appropriate standards.

Nevertheless, in applying IP law norms, the *Compulife* standards ask the appropriate questions, allowing courts to find the optimal balance between database protection and societal interests in disseminating information. The *Compulife* theory is also comparable to the EU *sui generis* database right. Both doctrines address the same problem—the inadequate copyright protection of databases. This Note argues that *Compulife* is a step in the right direction—a step towards recognizing a *sui generis* database right.

It is unclear how far *Compulife* extends and whether other courts will adopt it.[316] Nevertheless, this Note advocates for the adoption of *Compulife* and the embrace of trade secret law to approach data scraping cases. A broad acceptance of *Compulife* would usher in a new conceptualization of intellectual property rights in databases.

[316] On remand from the Eleventh Circuit's decision in *Compulife*, the district court found the scraping to be improper means and ultimately found the defendant liable for trade secret misappropriation. *Compulife Software, Inc. v. Rutstein*, No. 9:16-CV-80808, 2021 WL 3713173, at *20–21 (S.D. Fla. July 12, 2021), *order clarified*, No. 9:16-CV-80808-BER, 2021 WL 5830554 (S.D. Fla. Oct. 20, 2021). The court found that "so much of the [insurance quote] Database was taken during the scraping attack that it amounted to a protected portion of Compulife's trade secret." *Id.* at *20. The court stated: "I find that by using a robot to hack [Compulife's] website, Defendants intentionally sought to acquire Compulife's trade secrets through improper means. Defendants' subsequent use of the [] website in a way that was never intended, stealing a significant portion of Compulife's data, and knowingly incorporating that stolen data into its own websites also constitutes improper means." *Id.* at *21.