DATABASE PROTECTION, DATA PORTABILITY, SCREEN SCRAPING AND THE USE OF CONTENT AND DATA FOR MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

From the forthcoming 2023 update to Chapter 5 (Database Protection, Data Portability, Screen Scraping and the Use of Content and Data for Machine Learning and Artificial Intelligence)
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

PRIVACY & CYBERSECURITY LITIGATION YEAR IN REVIEW

PRIVACY AND CYBERSECURITY SECTION

OF THE LOS ANGELES COUNTY BAR ASSOCIATION

JANUARY 19, 2023

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles:	Silicon Valley:	Washington, D.C.:
1840 Century Park East, Ste. 1900	1900 University Avenue, 5th Fl.	2101 L Street, N.W., Ste. 1000
Los Angeles, CA 90067	East Palo Alto, CA 914303	Washington, D.C. 20037
Direct Dial: (310) 586-6575	Direct Dial: (650) 289-7881	Direct Dial: (202) 331-3138
Direct Fax: (310) 586-0575	Direct Fax: (650) 462-7881	Fax: (202) 331-3101

Ballon@gtlaw.com
<www.ianballon.net>
LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West 2023 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net

GT GreenbergTraurig

Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal Circuits
U.S. Supreme Court

JD, LLM, CIPP/US

Ballon@gtlaw.com
LinkedIn, Twitter, Facebook: IanBallon

Los Angeles
1840 Century Park East
Suite 1900
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Silicon Valley
1900 University Avenue
5th Floor
East Palo Alto, CA 94303
T 650.289.7881
F 650.462.7881

Washington, D.C.
2101 L Street, N.W.
Suite 1000
Washington, DC 20037
T 202.331.3138
F 202.331.3101

Ian C. Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and AdTech class action suits.

Ian has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2022). He has been listed in Best Lawyers in America consistently every year since 2003 and was named Lawyer of the Year for Information Technology in 2023, 2022, 2020, 2019, 2018, 2016 and 2013. In 2022, 2021, 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In 2022, Ian was named to Lawdragon's list of the Top 500 Lawyers in America and he has been included on the *Daily Journal's* annual list of the Top 100 Lawyers in California. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal and he has been* recognized as a "Groundbreaker" in *The Recorder*'s 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's Vanguard Award for significant contributions to the development of intellectual property law. Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named a Northern California Super Lawyer every year from 2004 through 2021 and a Southern California Super Lawyer for every year from 2007-2021. He has also been listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian is also the author of the leading treatise on internet and mobile law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). In addition, he serves as Executive Director of Stanford University Law School's Center for the Digital Economy. He also chairs PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian holds JD and LLM degrees and the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 1

THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

Chapter 5

Database Protection, Data Portability, Screen Scraping, and the Use of Content and Data for Machine Learning and Artificial Intelligence

5.01 Database Law, Access Rights, and the Automated Means Used to Extract, Compile and Analyze Data—In General

Data and information contained in databases or stored online may be protected from third party use in the United States to varying degrees by a smorgasbord of state and federal laws that may apply, depending on the nature of the database and ways in which it is protected, the type of infor-

mation (whether publicly available or proprietary, factual or creative), how the data or content was accessed, and what is being done with it. The specific requirements to state a claim under potentially applicable laws, and an array of defenses—including fair use, statutory exceptions and various preemption doctrines—potentially limit a database owner's ability to protect its data and information from unwanted third party use. For these reasons, data or screen scraping[1]—or the practice of automatically extracting unprotectable facts or other data from third party websites or other locations—if done correctly, is permissible in certain instances. The variety of fact-specific claims and defenses, and evolving circuit splits in some areas of potentially applicable law, make database protection and screen scraping an area where close adherence to the law, and how it is developing, is important. It is also an area where missteps, by either database owners or screen scrapers, can have significant consequences. This chapter addresses the various claims and defenses potentially applicable and provides practical checklists[2] for database owners seeking to protect their data and those engaged in lawful scraping (including through the use of artificial intelligence). It also addresses E.U. law on database protection.[3]

In addition to considering proprietary and access rights to data and information, this chapter addresses the automated means employed for extracting data online, through the use of bots or intelligent agents to scrape data or other information from databases. The flipside to thin database protection is that competitors and others may, subject to the various laws analyzed in this chapter, freely access data that is not protected through the various means outlined in this chapter. Businesses typically use bots or intelligent agents to automatically search for and retrieve particular data. The legal regime is largely the same regardless of whether the software agents are preprogrammed to perform a routine task, intelligent agents that are programmed to make decisions, or agents using machine learning or artificial intel-

---

[Section 5.01]

[1]*Scraping* is the programmed extraction of data, usually by a bot or intelligent agent software (often referred to as a *screen scraper*), as opposed to manual copying.

[2]*See infra* §§ 5.13, 5.14.

[3]*See infra* § 5.10.

ligence (referred to generally as AI). In all cases, the company that deployed the agent is likely to be liable for any misconduct, much in the same way that a business is responsible for any misconduct by an employee acting within the scope of employment. This liability may be varied by contract or subject to indemnification obligations or insurance, but the party that deployed an agent in most cases, absent a statutory or contractual provision to the contrary, likely will be liable for the actions it directed, preprogrammed, or enabled through AI. IP aspects of AI are addressed throughout this chapter and in section 5.15.

Internet businesses may seek access to third party data, even as they seek to protect their own data from third party exploitation. While much data and information is closely held, vast databases of information may be accessed online through publicly available websites or mobile apps or from subscription services. Databases are electronic compilations of information. Companies such as Reuters, Reed-Elsevier, Inc., Dow Jones and Dun & Bradstreet spend large sums compiling original databases of useful information that are typically made available to subscribers for monthly or other periodic access fees or charges for specific content in the database, such as a reprint of a single article. The legal protection afforded database content in the United States, however, is limited. Unless a database is comprised of material that itself is independently entitled to copyright protection (such as photographs, articles, music files or video clips), the level of copyright protection for a compilation of otherwise unprotectable material (such as a factual database) likely will be thin. In such cases, database owners may need to rely on a patchwork of other remedies, each one of which typically provides only narrow and limited relief which may or may not protect a database owner in a given case, as laid out in this chapter.

The 1976 Copyright Act created a split copyright interest in compilations.[4] The owner of a database, which is a compilation of facts or other content, potentially may be

[4]*See* 17 U.S.C.A. § 201(c); *see generally supra* § 4.05[3]. A *compilation* is a work "formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship. The term 'compilation' includes collective works." 17 U.S.C.A. § 101. A *collective work* is "a work, such as a periodical issues, anthology, or encyclopedia, in which a number of contributions, constituting separate

entitled to a copyright in the database itself, provided there is sufficient creativity in the selection, arrangement, or organization of the database to merit copyright protection. In addition, the owner or owners of the contributions to the collective work—which could be the same as the owner of the database or could be different people—retain a copyright in their individual contributions, if protectable. Thus, for example, freelance authors who contributed articles to a newspaper may retain their individual copyrights in the articles while at the same time the newspaper may register a copyright for the compilation that includes those articles (for example, the December 5th edition of *The Miami Herald*). In the absence of an express transfer of the copyright to a contribution to a collective work, the owner of the collective work (in this case, the database) is presumed to have acquired only the privilege of reproducing and distributing the contribution as part of that particular collective work (the December 5th edition), any revision of that collective work (such as the afternoon edition) and any later collective

---

and independent works in themselves, are assembled into a collective whole." *Id.*

In evaluating whether something is a compilation, the Ninth and Eleventh Circuits consider that how material is registered—as individual works or a compilation—will not be controlling, but may be considered as a relevant factor. *See VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 748 (9th Cir.) (*citing Yellow Pages Photos, Inc. v. Ziplocal, LP*, 795 F.3d 1255, 1277 (11th Cir. 2015) ("Although the manner of copyright registration is not dispositive of the works issue, this Court has previously considered it to be at least a relevant factor.")), *cert. denied*, 140 S. Ct. 122 (2019); *see also VHT, Inc. v. Zillow Group, Inc.*, 461 F. Supp. 3d 1025, 1040-45 (W.D. Wash. 2020) (holding, on remand, that the VHT images at issue were not part of a compilation as a matter of law, where VHT registered the images both individually and as part of a database compilation and the images individually had independent economic value, thus entitling VHT to recover multiple statutory damage awards, rather than merely a single award, for Zillow's inclusion of the images in its real estate database; ruling that Zillow's use of plaintiff's images as part of a single database of real estate listings was irrelevant, because whether images in a database constitute one work or many depends on how the copyright owner treated the material when it was released to the public, not how the accused infringer used it).

Works first published prior to January 1, 1978, are not subject to the 1976 Copyright Act and therefore are not be subject to the split copyright created by section 201(c) for works created on or after January 1, 1978. For a more complete discussion of the scope of section 201(c) and potential *Tasini* issues, *see infra* § 17.03.

work in the same series.[5]

In *New York Times Co. v. Tasini*,[6] the U.S. Supreme Court ruled that digitized versions of a newspaper were not "revisions" as that term is used in section 201(c) of the Copyright Act. Thus, freelance authors who had granted permission to *The New York Times* to include their works in the original editions of the paper and, by operation of law, "any revision . . . , and any later collective work in the same series" but who had retained their separate copyright in their articles (or "contributions" to the collective work), were deemed not to have authorized *The New York Times* to reproduce digitized versions of their articles in electronic databases. *Tasini* underscores that different parties may own rights to creative content in a compilation such as a database—such as articles, photographs, music files and the like—and, if so, the owner of the compilation may need to obtain express permission from the owner of a contribution to a collective work when the collective work is reused in new media (such as when preexisting works are included in an electronic database).[7]

By contrast, when a database is comprised of factual information or content that is otherwise unprotectable—such as U.S. government publications or court opinions—there is only one copyright potentially at issue. A database that is a compilation of unprotectable data or information may be subject to copyright protection if there is creativity in the selection, arrangement or organization of the database.[8] The level of copyright protection, however, is thin, and may not protect the owner against all forms of copying.

Since the U.S. Supreme Court's rejection of the "sweat of the brow" doctrine in 1991 in *Feist Publications, Inc. v. Ru-*

---

[5]17 U.S.C.A. § 201(c).

[6]*New York Times Co. v. Tasini*, 533 U.S. 483 (2001).

[7]*See supra* § 4.05[3] (discussing *Tasini* and subsequent cases); *infra* § 17.03 (discussing licensing issues arising out of *Tasini*).

[8]A database is a software application and therefore the application itself also may be entitled to copyright protection (as well as potentially patent or trade secret protection), but this legal protection for the software application will not protect the components of a database (although this additional copyright potentially could be used to prevent unauthorized access to the database). *See infra* § 5.03[1].

A database also may include personal information subject to privacy and security laws which are addressed in, respectively, chapters 26 and 27.

ral Telephone Service Co.,[9] the fact that a company may have invested significant time and money creating a database no longer assures it that its work will be protected by copyright law. Many commercial databases are literally large collections of unprotectable factual data efficiently organized to facilitate rapid search and retrieval.[10] Copyright protection may extend to the arrangement and selection of the data, if sufficiently creative, but not to the underlying data itself. While copyright law therefore may protect a database owner from piracy—when the entire database is literally copied and incorporated in a new work or posted at a different location—it typically does not prevent competitors from reviewing a database and copying unprotectable facts or data (so long as the extent of copying does not rise to the level where the competing work is substantially similar or virtually identical[11] to the work copied). Indeed, in many instances, it is possible to construct a minimally creative, noninfringing database that incorporates unprotectable facts copied from a rival.

In the process of extracting unprotected data from a website, a screen scraper sometimes must copy protectable content—such as software, photos or creative text or other expression. Scraping may occur in real time (where unprotectable data is extracted directly without making a full copy of the database or file in which the data was stored) or only after an entire database has been copied (if only briefly) and the sought-after factual material extracted. If an intermediate copy is made to allow extraction of unprotected material, it would constitute an unauthorized reproduction but could be deemed fair use intermediate copying if the entire copy is retained only briefly while factual or other unprotected information is extracted, and the copy is then promptly deleted,[12] depending on the ultimate use of the material extracted (and in particular whether it is transformative).

---

[9] *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991); *see generally supra* § 4.02; *infra* § 5.02.

[10] *See* Merriam-Webster's Collegiate Dictionary Deluxe Electronic Edition (1995) (defining a database as "a usually large collection of data organized especially for rapid search and retrieval (as by a computer).").

[11] A number of courts require a showing of virtual identicality or heightened substantial similarity in order to establish copyright infringement where the work is a compilation of primarily unprotectable elements and therefore entitled to thin copyright protection. *See infra* § 5.02.

[12] *See, e.g.*, *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510,

Other fair use principles also may weigh in favor of fair use when material is copied from a database,[13] although fair use is an affirmative defense so it would be the scraping party's burden to establish its applicability.

In Europe, unlike the United States, databases are entitled to *sui generis* protection analogous to copyright law.[14] U.S.

1520–28 (9th Cir. 1992); *Nautical Solutions Marketing, Inc. v. Boats.com*, 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121 (M.D. Fla. Apr. 1, 2004) (holding that "momentary copying of open . . . public Web pages in order to extract yacht listings facts unprotected by copyright law constitutes a fair use."); *Ticketmaster Corp. v. Tickets.com, Inc.,* CV99-7654-HLH (VBKx), 2003 WL 21406289, at *5 (C.D. Cal. Mar. 7, 2003) ("Taking the temporary copy of the electronic information [from the Ticketmaster.com website database] for the limited purpose of extracting unprotected public facts leads to the conclusion that the temporary use of the electronic signals was 'fair use' and not actionable."); *see also Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003) (citing *Sega* and other cases for the proposition that intermediate copying is a fair use where the only effect of enjoining it would be to give the copyright owner control over noninfringing material produced by a competitor, which was stated in *dicta* as a warning to the plaintiff to not attempt to circumvent the court's order by reconfiguring its product to make it impossible for customers to extract data without making unauthorized copies); *see generally supra* § 4.10[1] (analyzing intermediate copying as potentially but not always a fair use); *infra* § 5.02.

[13]*See generally infra* § 5.02[2]; *supra* § 4.10[1] (analyzing copyright fair use more extensively).

[14]In the mid-1990s, PTO Commissioner Bruce Lehman and others spearheaded efforts to create sui generis protection for databases much in the same way that Congress had created a new form of intellectual property protection for semiconductor chips in the early 1980s in the Semiconductor Chip Protection Act. *See* 17 U.S.C.A. §§ 901 *et seq*. In February 1996, the European Community submitted a proposal to WIPO for international harmonization of database laws, based on the EU Database Directive. *See* Jack E. Brown, "Proposed International Protection of Electronic Databases," The Computer Lawyer, Jan. 1997, at 17, 19. Similar protection would have been afforded to databases under the Database Investment and Intellectual Property Antipiracy Act, H.R. 3531, 104th Cong. 2d Sess. (1996), which was introduced in Congress in 1996, but not enacted. Critics of both initiatives argued that they would not merely reverse *Feist* with respect to databases, but grant broad sui generis protection to collections of otherwise unprotectable facts without the same fair use safeguards otherwise available under U.S. copyright law. *See supra* § 4.10 (analyzing copyright fair use). Critics also charged that the Clinton Administration had sought to have the essential provisions of the failed 1996 database bill made part of U.S. law through negotiation of an international database treaty which would then have been submitted to Congress a *fait accompli*. *See, e.g.,* Pamela Samuelson, "Big Media Beaten Back," Wired, Mar. 1997, at 61. The proposed treaty, however, was never

residents, however, typically cannot take advantage of this protection for their works in Europe, although it is possible to structure operations such that a European entity could obtain database protection for a work under EU law.[15]

In the absence of strong intellectual property protection, U.S. database owners seek to protect the content of their databases by contract. Contractual restrictions in subscription agreements or access licenses, however, only work where there is privity of contract (although potentially, claims could be asserted for interference with contract or prospective economic advantage, to the extent that a third party provides tools to allow a user to breach the database or website access agreement).[16] In addition, where purported licensing restrictions are merely posted on a site, assent may be deemed lacking and no contract formed.[17]

Database owners may be able to prevent screen scraping or copying from their databases under state unfair trade statutes or common law theories, such as misappropriation, to the extent not preempted by the Copyright Act, the Patent Act, the Lanham Act, or the Uniform Trade Secrets Act. State law claims based on copying information from a database will be preempted by the Copyright Act (and therefore be unavailable, even if copyright law itself provides no measure of relief because the material copied is merely factual data) unless the database owner can allege at least one additional element (beyond what would be required to state a claim for copyright infringement). If not preempted, databases that provide "hot news"—such as stock quotes or sports scores that have value for their timeliness—may be entitled to protection based on common law misappropriation if the act of copying information also involves the theft of lead time.[18] Where the only state law claim a party may assert is that data was merely copied, the claim likely will

---

approved by WIPO. In 1998, the Collection of Information Antipiracy Act, H.R. 2652, 105th Cong. 2d Sess. (1998), which included fair use provisions, was passed by the U.S. House of Representatives, but failed to win passage in the U.S. Senate. *See* David Mirchin, "Putting An End to Database Piracy," Boston Globe, June 2, 1998, at C4. Efforts to create sui generis database protection in the United States ultimately faded over time.

[15]*See infra* § 5.10.

[16]*See infra* § 5.03[5].

[17]*See infra* § 5.03.

[18]*See infra* § 5.04.

be deemed preempted by the Copyright Act.[19] In more limited circumstances, where the content of a database is also a trade secret, other state law claims may be preempted in states that have enacted section 7 of the Uniform Trade Secrets Act.[20] In even more limited circumstances, state law claims also could be preempted by the Patent Act, where state law presents an obstacle to the execution and accomplishment of patent laws or offers patent-like protection to intellectual property that is inconsistent with the federal scheme.[21] Claims against platforms, intermediaries or other interactive computer service providers based on user misconduct, or asserted against users for republishing or restricting access to or removing third party material, also may be preempted by the Communications Decency Act.[22]

A claim for trespass may be asserted where access to a database is unauthorized. Whether access is unauthorized may turn on the Terms of Use of a site or whether notice was provided. Most courts, however, require a showing of actual injury, such as diminishment of server capacity, which may be difficult to establish.[23] A database owner also may be able to sue for unauthorized access under the Computer Fraud and Abuse Act, an anti-hacking statute, if a minimum of $5,000 in damages may be shown[24] (or aggregated in a class action suit).[25] Where access restrictions are circumvented or copyright management information removed, claims potentially could also be brought under the Digital Millennium Copyright Act (DMCA).[26]

In narrow circumstances involving online event ticket sales, the Better Online Ticket Sales Act (or BOTS Act)[27] makes it unlawful to "circumvent a security measure, access control system, or other technological control or measure on an Internet website or online service that is used by the ticket issuer to enforce posted event ticket purchasing limits

---

[19] *See infra* § 5.04.

[20] *See infra* §§ 5.09, 10.17.

[21] *See infra* § 5.04[3].

[22] *See generally infra* § 37.05.

[23] *See infra* § 5.05.

[24] *See infra* § 5.06.

[25] *See infra* § 44.08.

[26] *See infra* § 5.07.

[27] *See* 15 U.S.C.A. § 45c.

or to maintain the integrity of posted online ticket purchasing order rules . . . ."[28]

Likewise, in narrow circumstances, California's BOT Disclosure Law[29] prohibits the undisclosed use of bots to communicate or interact with a person in California online, with the intent to mislead the other person about the artificial identity of the bot, to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election.

Where material scraped or copied includes logos or other branding, a claim potentially may be asserted under the Lanham Act.[30] Some Lanham Act claims may be preempted, however, under the U.S. Supreme Court's decision in *Dastar Corp. v. Twentieth Century Fox Film Corp.*,[31] which could preclude claims where branding information or credits are edited out of material from a factual database or other compilation that is unprotectable, if the Lanham Act claim (or potentially even a state law unfair competition cause of action) amounts to a disguised copyright claim.[32]

A claim also potentially could be brought for trade secret misappropriation, but only where the contents of a database are secret.[33] As previously noted, however, where the information at issue is a trade secret (and in some jurisdictions, even if it is not protectable as a trade secret), other state law claims, such as common law misappropriation, may be preempted under the laws of those states that have enacted section 7 of the Uniform Trade Secrets Act.[34]

Claims asserted against third parties for merely republishing or hosting material (such as advertisements or promotional material for screen scraping tools), as opposed to those directly responsible, or for restricting access to objectionable material, may be preempted by the Good Samaritan Exemption to the Telecommunications Act of 1996 (called colloqui-

---

[28]15 U.S.C.A. § 45c(a)(1)(A); *see generally infra* § 5.07[3].

[29]Cal. Bus. & Prof. Code §§ 17940 *et seq.*; *infra* § 5.16.

[30]*See infra* § 5.08.

[31]*Dastar Corp. v. Twentieth Century Fox Film Corp.*, 539 U.S. 23 (2003); *see generally infra* § 5.08.

[32]*See infra* § 5.08.

[33]*See infra* § 5.09.

[34]*See infra* § 5.09.

ally the Communications Decency Act, or CDA).[35]

In short, the remedies potentially available to database owners under U.S. law tend to be narrow and shallow. Absent copyright protection for the components of a database, an owner's copyright in the database itself, as a factual compilation, will only restrict literal copying that rises to the level of substantial similarity or virtual identicality. Protection may be augmented by contract, but only if the actual agreement is binding and not unconscionable. Some courts also are reluctant to enforce either copyright or contract rights that effectively prevent access to material in the public domain. Contract claims likewise may be unavailable in the absence of privity of contract, although a party engaging in screen scraping (or providing its users with the tools to do so) potentially could be sued for tortious interference with contract or prospective economic advantage in some circumstances. Common law misappropriation provides very specific grounds for relief, but only where a claim is not preempted, such as when based on the timeliness of the delivery of information, rather than mere copying. Trespass may be a viable claim where a party accesses a site without authorization, but generally requires a showing of damage to the chattel (not merely a business or competitive injury), such as diminishment of server capacity. The Computer Fraud and Abuse Act may provide relief premised, like trespass, on unauthorized access, but only if a minimum of $5,000 in damage may be shown. The anti-circumvention provisions of the Digital Millennium Copyright Act may afford additional remedies, but only where copy protection or access controls are circumvented or copyright management information is removed. The Better Online Ticket Sales (BOTS) Act proscribes circumventing a security measure, access control system, or other technological control or measure that is used by a ticket issuer to enforce posted event ticket purchasing limits or to maintain the integrity of posted online ticket purchasing order rules. A claim may be brought under the Lanham Act where a brand is copied or tarnished in connection with screen scraping, but the Lanham Act does

---

[35] 47 U.S.C.A. § 230(c); *see generally infra* § 37.05. As analyzed in section 37.05[5][B], certain claims pertaining to intellectual property, among others, are excluded from the scope of the exemption.

While the CDA potentially provides immunity based on data or content originating with a third party, it does not insulate a party from its own direct liability for any act or omission.

not prohibit copying of underlying data. Similarly, relief may be obtained for misappropriation of trade secrets, but only in those instances where a database is comprised of confidential information treated as a trade secret. While one or more of these remedies may suffice to provide relief in a given case, in many instances a screen scraper can structure its conduct to avoid liability under this patchwork of remedies.

Without careful planning, however, those seeking to access, analyze or otherwise use third party data may run afoul of laws that afford substantial statutory damages (such as the Copyright Act and DMCA, if applicable) or which otherwise may permit database owners to file suit to seek injunctive relief or prove actual damages. Even where no law is violated or where damages may be difficult to prove, the public relations aspect of a lawsuit may adversely impact a company if its practices are viewed as unfair, harsh or dishonest in the court of public opinion.

Beyond legal remedies, database owners may employ technological and other means to prevent access to their sites or services or to terminate users who violate their subscription agreements or otherwise use their data in undesirable ways. Where access is denied, it may prove challenging for parties to compel a database owner to allow scraping to continue.[36] Those denied access have sought, among other things, to allege antitrust violations[37] or unfair competition claims, although most such claims have been

---

[36]*See, e.g.*, *Facebook, Inc. v. BrandTotal Ltd.*, Case No. 20-cv-07182-JCS, 2021 WL 662168 (N.D. Cal. Feb. 19, 2021) (dsimissing BrandTotal's counterclaims for declaratory relief, interference with contract, and unfair contract); *Facebook, Inc. v. BrandTotal Ltd.*, 499 F. Supp. 3d 720 (N.D. Cal. 2020) (denying BrandTotal's motion for a temporary restraining order, in a case where the defendant alleged that it merely provided data analysis services to clients about their own advertising). *Cf. hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (affirming the lower court's preliminary injunction barring LinkedIn from denying access to hiQ to publicly available user data posted on its website under the Computer Fraud and Abuse Act, without addressing remedies that might be available under other laws, and even as the appellate court acknolwedged that LinkedIn could take measures to "thwart denial-of-service attacks and block[] abusive users, identity thieves, and other ill-intentioned actors[,]" noting that the district court had made clear that the injunction did "not preclude LinkedIn from continuing to engage in 'technological self-help' against bad actors—for example, by employing 'anti-bot measures to prevent, *e.g.*, harmful intrusions or attacks on its server.' "); *see generally infra* § 5.06 (analyzing hiQ and the CFAA).

[37]*See, e.g.*, *hiQ Labs, Inc. v. LinkedIn Corp.*, 485 F. Supp. 3d 1137

unsuccessful to date. Antitrust is separately analyzed in chapter 34. Unfair competition claims, which may be asserted both against those engaged in screen scraping and data acquisition (to the extent not preempted by the Copyright Act), or against those seeking to restrict data portability, is analyzed in section 5.04.

Issues raised by the Cybersecurity Information Sharing Act (CISA)[38] are summarized in section 5.12 and analyzed in more depth in section 27.04[1.5] in chapter 27.

A checklist of potential issues for rights owners and others is set forth in section 5.13. A form for proposed injunctive relief is set forth in section 5.11. A checklist for ethical scraping practices is set forth in section 5.14. Section 5.15 addresses ownership and other IP rights when information and data is scraped or gathered, compiled, or analyzed using automated agents or AI. Data integrity, which is a concern to database owners and their commercial partners as well as to consumers, is considered in section 5.17.

While this chapter addresses the assertion of proprietary rights and restrictions on data portability by data owners and access rights by third parties, claims of ownership, scraping and the use of bots, machine learning and AI to gather information also implicate the privacy interests of those whose data may be accessed. Privacy and security issues related to personal information in databases are separately analyzed in chapters 26 and 27, respectively, including in section 26.03A on AI and privacy.

Consumer concerns about data held by commercial interests are likewise addressed primarily through data privacy and cybersecurity laws, which are analyzed in chapters 26 and 27, although they are also discussed briefly in section 5.17 in connection with data integrity.

5.02 Copyright Protection for Databases

5.02[1] Scope of Protection

While factual data generally is not entitled to copyright protection, scraping protected content, even in small quantities, may amount to copyright infringement if the portion

---

(N.D. Cal. 2020) (dismissing hiQ's antitrust claims against LinkedIn for failing to define a product market or adequately allege anticompetitive conduct); *see generally infra* §§ 34.01 *et seq.* (analyzing antitrust law).

[38] 6 U.S.C.A. §§ 1501 to 1510; *infra* § 27.04[1.5].

copied is not a fair use[1] and the copying is not otherwise permissible. For example, in *The Associated Press v. Meltwater U.S. Holdings, Inc.*,[2] the court held that a news aggregator's use of the lede, or introductory section of a news story that summarizes the story, which was automatically scraped from targeted sources, including Associated Press licensees, and included in Meltwater's subscription news summaries, was infringing and not a fair use or otherwise justified based on implied license, estoppel, copyright misuse or other defenses.[3]

Using bots to extract data from websites or databases may raise an array of issues. In *Ticketmaster LLC v. Prestige Entertainment West, Inc.*,[4] however, Ticketmaster sued the defendant for secondary copyright infringement,[5] arguing that the defendant's use of bots to extract data from the Ticketmaster site was so sophisticated that it necessarily had to have copied extensive portions of Ticketmaster's web content and code. Specifically, Ticketmaster alleged that (1) third party Bot Developers developed bots that proved highly

---

[Section 5.02[1]]

[1]Copyright fair use is analyzed in section 4.10[1].

[2]*The Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537 (S.D.N.Y. 2013).

[3]In rejecting Meltwater's fair use defense, the court held that the use of AP articles in Meltwater's news summaries was not transformative and that the summaries were substitutes for the genuine works, with subscribers clicking through to the AP articles only 0.08% of the time. The court found that the amount and substantiality of the portion taken also weighed against a finding of fair use because Meltwater's scraping tool automatically took the lede from every AP story (in either 140 or 300-character excerpts) which, depending on the length of the article, amounted to between 4.5% and 61% of a genuine work.

The court rejected Meltwater's implied license defense because consent to copy the lede could not reasonably be inferred from the AP's failure to affirmatively block crawlers using a robots.txt file. As the court explained, "what Meltwater is suggesting would shift the burden to the copyright holder to prevent unauthorized use instead of placing the burden on the infringing party to show it had properly taken and used content."

The court likewise rejected Meltwater's estoppel defense because the AP had no duty to restrict general access to its online content by requiring its licensees to put AP content behind a paywall nor did it have any duty to notify Meltwater that it objected to Meltwater's scraping before filing suit.

[4]*Ticketmaster LLC v. Prestige Entertainment West, Inc.*, 315 F. Supp. 3d 1147 (C.D. Cal. 2018).

[5]*See generally supra* § 4.11 (analyzing secondary infringement).

capable of purchasing large quantities of tickets on the Ticketmaster.com website, and (2) Ticketmaster's website and mobile app are complex platforms that each contain several layers of protection and security measures. Ticketmaster alleged that developing such capable bots would necessarily require deep study and analysis of the pages and code of Ticketmaster's website and mobile app, which meant that the Bot Developers must have downloaded and stored literal or non-literal elements of Ticketmaster's website and mobile app on their local systems in the course of developing these bots.[6] The court, in denying defendant's motion to dismiss, agreed that Ticketmaster had at least alleged a plausible claim of copyright infringement.[7]

When material is scraped or copied from a database, as discussed in section 5.01, there potentially may be two separate copyright owners of the contents of the database[8]—the owner of the collective work and, if different, the owner of contributions to that collective work.[9] A copyright in a compilation generally does not extend to preexisting works

---

[6]More specifically, Ticketmaster alleged that the bots enabled defendants to launch thousands of concurrent and recurring reserve requests for tickets for specific events. The bots were calibrated such that when the reserve request expired, the bot was able to regenerate a new ticket reserve request at a far greater speed than any legitimate human could manage, thus preventing any human from reserving or purchasing the ticket. Moreover, the bots could trade information so that purchases coming from multiple computers would appear to be coming from the same computer, allowing the bots to hide themselves by more closely mirroring what Ticketmaster's algorithms considered normal human use. Finally, the bots were able to escape detection when ordering tickets through the mobile app interface, which Ticketmaster alleged was not possible without first obtaining certain lines of code called security tokens embedded deep within the code of the Ticketmaster mobile app. *See Ticketmaster LLC v. Prestige Entertainment West, Inc.*, 315 F. Supp. 3d 1147, 1162-63 (C.D. Cal. 2018).

[7]*Ticketmaster LLC v. Prestige Entertainment West, Inc.*, 315 F. Supp. 3d 1147, 1159-66 (C.D. Cal. 2018).

[8]A database program, like the contents of a database, may also be entitled to copyright protection if original and creative. *See supra* § 4.07. As noted by one court, a "database is not simply a shoe box into which all information is thrown. It is, rather, a very structured hierarchy of information." *Positive Software Solutions, Inc. v. New Century Mortgage Corp.*, 259 F. Supp. 2d 531, 532 n.1 (N.D. Tex. 2003). A copyright in the underlying database software, however, generally will not protect against copying of contents stored in a database.

[9]*Tasini* problems—where the owners of contributions to the collective are different from the owner of the collective work and where ade-

included in the compilation, such as articles, photos, or other material. These components, if protectable, are separately copyrightable.[10] A copyright in a database, as a compilation, merely protects the selection, arrangement, or organization of the material in the database, to the extent sufficiently creative to be entitled to copyright protection.[11] Many databases are comprised of material that is not separately protectable under U.S. copyright law, such as factual information or data, court opinions, government records or other components in the public domain. As discussed in this section, protection for a database that constitutes a compilation of facts or otherwise separately unprotectable material is quite limited under U.S. copyright law, but is potentially available where there is creativity in the selection, arrangement, or organization of the compilation. A form for applying for copyright protection for a database is included in the appendix to chapter 4. By contrast, a database comprised of public domain records or other unprotectable material, where there is no creativity in the selection, arrangement, or organization of the database, will not be entitled to copyright protection, and claims based on scraping that database may be preempted by the Copyright Act (absent an "extra element" beyond mere copying).[12]

"Facts are not copyrightable, because they lack any degree

---

quate electronic rights have not been obtained—are addressed in section 5.01.

[10]*See* 17 U.S.C.A. § 103. Potential registration issues with database compilations are separately analyzed in section 4.08[2].

[11]*See* 17 U.S.C.A. § 103.

[12]*See, e.g.*, *Citizens Information Associates, LLC v. Justmugshots.com*, Civil No. 1-12-CV-573-LY, 2013 WL 12076563, at *3 (W.D. Tex. Feb. 26, 2013) (dismissing BustedMugshots.com's state law claims as preempted by the Copyright Act where the plaintiff aggregated millions of publicly available arrest records on its website, which had been scraped by a competitor, JustMugShots.com); *Citizens Information Associates, LLC v. Justmugshots.com*, Civil No. 1-12-CV-573-LY, 2012 WL 12874898 (W.D. Tex. Dec. 18, 2012) (denying plaintiff's motion for a preliminary injunction where it alleged that the defendant scraped over 14 million arrest records from its website, which defendant argued he was free to do because the records were in the public domain, even though the plaintiff expended significant sums compiling the database and keeping it current, because plaintiff was not likely to prevail on the merits and the public interest did not favor enjoining the dissemination of public records); *see generally supra* § 4.18[1] (analyzing copyright preemption); *infra* § 5.04[1] (addressing copyright preemption in connection with database protection/ scraping claims based on misappropriation).

of creativity. . . . Facts exist and are not created."[13] Purely factual compilations involving no creativity in the selection, arrangement, or organization of data (such as telephone white page directories) are not entitled to copyright protection, since "raw facts may be copied at will."[14] Thus, for example, in *ProCD, Inc. v. Zeidenberg*,[15] the Seventh Circuit agreed with the lower court's analysis that a factual database that the defendant made available over the Internet was not entitled to copyright protection, where the database had been copied entirely from the plaintiff's CD-ROMs, which in turn contained telephone directory listings from all of the white pages published in the United States.[16]

Similarly, in *National Basketball Association v. Motorola, Inc.*,[17] the Second Circuit held that the transmission by pager of continuously updated basketball scores did not constitute copyright infringement because the defendants reproduced only facts from the protected broadcasts (the actual scores), "not the expression or description of the game that constitutes the broadcast."[18] Randomly generated codes[19] and the volume and page numbers assigned to otherwise unprotect-

---

[13]*Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176, 1181 (9th Cir. 2018).

[14]*Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 350 (1991). In *Feist*, the Supreme Court rejected the "sweat of the brow" doctrine, holding that hard work in creating a compilation is insufficient to confer copyright protection if the work does not contain the requisite level of creativity to meet statutory requirements. Facts, the Supreme Court emphasized, "do not owe their origin to an act of authorship . . ." and are "not 'original' in the constitutional sense." *Id.* at 347-48. Facts, whether "scientific, historical, biographical, or news of the day" are merely "discovered" or "record[ed]" and are not copyrightable. *Id.* at 347. While facts are unprotectable, a compilation may be protectable if it has "a minimal degree of creativity" in the "selection and arrangement" of the facts, but the level of protection for a factual compilation is "thin." *Id.* at 348-49.

[15]*ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

[16]The Seventh Circuit found for the plaintiff based on the enforceability of a consumer software license, and therefore did not extensively address the copyright issue. For an analysis of the case, *see infra* §§ 21.02, 21.03.

[17]*National Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841 (2d Cir. 1997).

[18]*National Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841, 847 (2d Cir. 1997).

[19]*See Mitel, Inc. v. Iqtel, Inc.*, 124 F.3d 1366, 1373 (10th Cir. 1997).

able information[20] likewise have been held to lack sufficient originality to be deemed protectable.

In *Bikram's Yoga College of India, L.P. v. Evolution Yoga, LLC*,[21] the Ninth Circuit held that copyright protection could not be obtained for Bikram Yoga's sequence of twenty-six asanas and two breathing exercises, arranged in a particular order, which the plaintiff called the "Sequence." The court explained that "[c]opyright protects only the expression of this idea—the words and pictures used to describe the Sequence—and not the idea of the Sequence itself. Because the Sequence is an unprotectible idea, it is also ineligible for copyright protection as a 'compilation'."[22]

While facts generally are unprotectable, in limited circumstances, "creative facts"—or "facts" derived from original, creative expression—may be found independently protectable, at least in the Second Circuit.[23] Study questions used in a film course likewise have been held to meet the minimal threshold of originality to be deemed protectable.[24]

Final values, or the products of formula or calculation, also potentially may be protected in limited circumstances.

---

[20]*See Matthew Bender & Co. v. West Publishing Co.*, 158 F.3d 693 (2d Cir. 1998) (star pagination unprotectable), *cert. denied,* 526 U.S. 1154 (1999). *But see Oasis Publishing Co. v. West Publishing Co.*, 924 F. Supp. 918 (D. Minn. 1996); *see also Thomson Reuters Enterprise Centre GmbH v. ROSS Intelligence Inc.*, __ F. Supp. 3d __, 2021 WL 1174725, at *1-7 (D. Del. 2021) (denying defendant's motion to dismiss plaintiffs' copyright infringement suit which alleged that ROSS used bots to scrape the Westlaw database, including "volumes of proprietary material (such as West Headnotes, case summaries, and other Westlaw-created content [including the West Key Number System])," to develop ROSS's own artificial intelligence-based legal search product).

[21]*Bikram's Yoga College of India, L.P. v. Evolution Yoga, LLC*, 803 F.3d 1032 (9th Cir. 2015).

[22]*Bikram's Yoga College of India, L.P. v. Evolution Yoga, LLC*, 803 F.3d 1032, 1036 (9th Cir. 2015).

[23]*See Castle Rock Entertainment, Inc. v. Carol Publishing Group, Inc.*, 150 F.3d 132 (2d Cir. 1998) (holding defendants liable for copyright infringement for creating the SAT (Seinfeld Aptitude Test), a trivia quiz book which tested readers' recollection of facts from the fictional television series *Seinfeld*; "unlike the facts in a phone book, which 'do not owe their origin to an act of authorship,' . . . each 'fact' tested by the SAT is in reality fictitious expression created by Seinfeld's authors . . . . [The] characters and events spring from the imagination of Seinfeld's authors . . . .").

[24]*See Faulkner Press, LLC v. Class Notes, LLC*, 756 F. Supp. 2d 1352, 1357 (N.D. Fla. 2010). The court explained:

In holding that settlement prices—or the value at the end of the trading day of a particular futures contract for a particular commodity for future delivery at a particular time—were not entitled to protection because, based on the merger doctrine,[25] the idea of the fair market value of contracts and their settlement value were essentially the same thing, the Second Circuit, in *New York Mercantile Exchange, Inc. v. IntercontentalExchange, Inc.*,[26] addressed, without deciding, the threshold issue of whether settlement values could, in the first place, even be found sufficiently original to be deemed protectable, explaining that:

> ["]The first person to find and report a particular fact has not created the fact: he or she has merely discovered its existence." . . . [For] example, census takes are not authors of the census data. Census takers merely discover the appropriate population figure; "in a sense, they copy these figures from the world around them." . . . The question then, is one of characterization: does the Committee create the settlement prices, or is it more accurate to view the Committee's task as like that of a census taker, copying the market's valuation of futures contracts? While the line between creation and

---

> Although the fact statements are taken from the various films Dr. Moulton showed in class and his questions track the sequence of the films, Dr. Moulton picked only a few facts from each film to include in his film study questions. There may be nothing innovating or surprising about his selection. His selection was possibly random and made solely to ensure that his students were paying attention to the films. Even so, the selection was original because it was not a mechanical or routine arrangement. Dr. Moulton's selection was unique to himself and unlikely to be duplicated by someone else tasked with compiling film study questions. Some creativity was involved. His selection therefore qualifies for copyright protection.

Id.

[25]Under the merger doctrine, material will be deemed unprotectable where there are so few ways to express an idea that the idea and expression may be said to have merged. *See, e.g.*, *New York Mercantile Exchange, Inc. v. IntercontinentalExchange, Inc.*, 497 F.3d 109, 116–18 (2d Cir. 2007); *Lathan v. City of Whittier Alaska*, Case No. 3:10-cv-00070, 2011 WL 13115649, at *10-11 (D. Alaska Aug. 4, 2011) (granting summary judgment where plaintiff's method for estimating the power output of a proposed hydropower project from raw data, even if sufficiently original to be potentially entitled to copyright protection, was unprotectable under the merger doctrine); *see generally supra* §§ 4.02 (analyzing the merger doctrine and protectability under the Copyright Act), 4.07 (copyright protection for software code).

[26]*New York Mercantile Exchange, Inc. v. IntercontinentalExchange, Inc.*, 497 F.3d 109 (2d Cir. 2007), *cert. denied,* 522 U.S. 1259 (2008).

> discovery is often clear-cut, we recognize that it is a difficult line to draw in this case.[27]

Summarizing earlier case law, Judge Karas of the Southern District of New York explained, in *BanxCorp v. Costco Wholesale Corp.*,[28] that the final value produced by a formula is unlikely to be entitled to copyright protection where (1) the raw data used to create the final value was comprised of unprotectable facts; (2) the method of converting raw data into the final value was an industry standard, or otherwise widely accepted as an objective methodology;[29] and (3) the

---

[27]*New York Mercantile Exchange, Inc. v. IntercontinentalExchange, Inc.*, 497 F.3d 109, 114 (2d Cir. 2007), *quoting Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 344, 347 (1991). In *Mercantile Exchange*, the plaintiff had obtained a copyright registration certificate for its database but could not, as a result of the court's holding, prevent an Internet competitor from copying individual settlement values.

The court did not decide whether settlement values contained sufficient originality to be protectable (holding that even if they did, any claim to protection was barred by the merger doctrine). The court explained the process of arriving at settlement values as follows:

> A futures contract requires the delivery of a commodity at a specified price at a specified future time, though most contracts are liquidated before physical delivery occurs . . . . [S]ettlement prices are used to value the open positions . . . . Unlike on a securities exchange, the settlement price may not be the final trade, for two reasons. First, because of the nature of trading, it is not always clear which trade was the closing trade . . . . Second, . . . [f]or the "outer" months, those further from the trading date, there is often little or no trading on a particular day . . . . For high-volume months, settlement prices are based on a formula: "a weighted average of all trades done within the closing range." . . . For low-volume months, the extent of the . . . creative judgment is disputed.

497 F.3d at 110–11. The majority wrote, in *dicta*, that there was "a strong argument" that settlement prices were unprotectable facts, *id.* at 114, although that argument was weaker for low-volume months, noting that if there was no real market in those months the settlement prices appeared closer to creations (or predictions of expected value). *See id.* at 116. In high volume months, by contrast, settlement values were "determinations of how the market values a particular futures contract . . . not how the market should value them or will value them . . . . So characterized, there is one proper settlement price; other seemingly-accurate prices are mistakes which actually overvalue or undervalue the futures contract." *Id.* at 115; *see also Woods v. Resnick*, 725 F. Supp. 2d 809 (W.D. Wis. 2010) (holding finance formulas used for financing automobiles were not copyrightable under the merger doctrine and as *scenes a faire*).

[28]*BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596 (S.D.N.Y. 2010).

[29]The court explained that

> if a scientist knew an object's mass and the force acting upon the object, this raw data could be converted into the object's acceleration due to that force by

final value attempted to measure an empirical reality.[30]

Stated differently, Judge Karas explained that to demonstrate that the final values produced by raw data are protectable under copyright law, a plaintiff must show one of the following three things: (1) the raw data used to create the final value was protectable; (2) the method of converting the raw data into a final value was an original (but not necessarily novel) process that is neither widely accepted as objective, nor an industry standard; or (3) the final value did not attempt to measure an empirical result.[31]

---

using the "formula" known as Newton's Second Law of Motion. This use of a formula would merely discover an "empirical reality." On the other hand, "formulae" that purport to identify the best baseball player based on some weighted composition of batting average, on-base percentage, defensive efficiency, and a myriad of other selective factors, are not discovering "empirical realities." The difference lies in the originality of the method used to compile or analyze the data.

BanxCorp v. Costco Wholesale Corp., 723 F. Supp. 2d 596, 603 (S.D.N.Y. 2010). The court emphasized that significant weight should be attached to the degree of consensus and objectivity that attaches to the formula. *Id.* "Though at first counter-intuitive, . . . the more acceptance a financial measure obtains (i.e., the more successful it is), the more 'fact-like' it becomes. Just as scientific theories start as mere speculation and eventually gain a patina of objectivity, economic indicators that we now rely upon, such as CPI, were once just glimmers in the eyes of economists." *Id.* at 605 n.7. At the same time, "the formula chosen can be generally accepted and objective enough to constitute a 'fact' without being completely accurate." *Id.* at 604 n.4 (noting that even Newton's Second Law of Motion is inaccurate because it fails to account for Einstein's theory of relativity).

[30] *BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 604–05 (S.D.N.Y. 2010), *citing New York Mercantile Exchange, Inc. v. IntercontinentalExchange, Inc.*, 497 F.3d 109 (2d Cir. 2007), *cert. denied,* 522 U.S. 1259 (2008), and *RBC Nice Bearings, Inc. v. Peer Bearing Co.*, 676 F. Supp. 2d 9 (D. Conn. 2009).

[31] *BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 605 (S.D.N.Y. 2010). Based on these tests, Judge Karas held that BanxCorp's National Average Money Market and CD Rates were unprotectable but that the method of converting raw data to final values involved sufficient minimal originality to be entitled to copyright protection.

Judge Karas found that there were potentially three levels of generality at which plaintiffs could be alleging copyright infringement—raw data, the product of the raw data (the actual averages listed in the BanxQuote Indices, or final value) and the arrangement and presentation of the final values (which he called the "arrangement."). *Id.* at 602. He characterized both the final value and arrangement as compilations. *See id.* As an illustration, Judge Karas described a hypothetical involving three banks, banks A, B and C, which charged interests rates of 4%, 5% and 6%, respectively, on a given type of account. "These facts are the raw data. The average of these rates, 5%, is the final value. The table or graph

containing this, and other, final values, is the arrangement." *Id.* at 602 n.2.

The court found that the underlying raw data was comprised of unprotectable facts about interest rates charged by certain banks and a variety of economic indicators, akin to the actual trade values at issue in New York Mercantile and the physical characteristics of ball bearings in RBC Nice Bearings, and therefore unprotectable. Similarly, the court found that the BanxQuote Indices were intended to measure, among other things, rates paid by investors on negotiable certificates of deposit and high yield savings accounts, which were objective facts about the banking market and akin to the attempt to measure the value of settlement prices as they are (not as they should or will be) in New York Mercantile or the radial strength of ball bearings in RBC Nice Bearings, and therefore the final values were unprotectable.

By contrast, the court found that the plaintiffs had stated a claim based on the method of converting the raw data to final values because, for purposes of a motion to dismiss, it was plausible to infer that the BanxQuote Indices did not contain simple mathematical averages, but were instead created through judgment being applied to disparate indicators. Among other things, plaintiffs alleged that they exercised discretion over exactly which values to use from within certain categories of indicators (such as "leading banks."). For purposes of stating a claim, the court held that the allegations were "sufficient to get Plaintiffs to first base." *Id.* at 607. Finally, the court found that the merger doctrine did not bar plaintiffs' claim because it was not implausible that the BanxQuote Indices were sufficiently subjective that a wide range of potential final values were possible. *Id.* at 608–09.

Unlike *New York Mercantile* and *RBC Nice Bearings*, *BanxCorp* was decided on a motion to dismiss, rather than a motion for summary judgment, so the court focused on facts alleged, rather than actual evidence.

In a subsequent opinion, however, in considering the evidence in ruling on competing motions for summary judgment, Judge Karas held that final values were unprotectable as facts, tables of weekly averages of interest rates offered by banks were not copyrightable as compilations and the merger doctrine rendered plaintiff's list of national average rates of interest offered by banks for given financial products unprotectable under the Copyright Act. *BanxCorp v. Costco Wholesale Corp.*, 978 F. Supp. 2d 280, 292-312 (S.D.N.Y. 2013).

Based on the evidence presented, the court determined that BanxCorp's national interest rate averages were calculated using simple mathematical averages of reported rates from major banks, with no weighting or other calculations involved. *Id.* at 294. The output of the calculation was a single number that was "the exact mathematical average of the inputted rates as of a particular date." *Id.* at 298. The averages were called "benchmark rates" or "national average rates," were described as "current," "accurate," and "true," and were represented to consumers, customers, and the financial media . . . [as] objective facts about average national interest rates as of a particular date." *Id.* at 298-99.

Citing *dicta* in *New York Mercantile*, Judge Karas explained that "when confronted with raw data that have been converted into a final

value through the use of a formula, courts should put significant weight on the degree of consensus and objectivity that attaches to the formula to determine whether the final value is fundamentally a 'fact.' " *Id.* at 300. Judge Karas elaborated that "[i]f the data purports to represent actual objective prices of actual things in the world—the actual price of an actual settlement contract on a particular day—it is an unprotectable fact; if the data purports to represent an estimated price of a kind of idealized object—for instance, what a hypothetical mint condition 2003 Ford Taurus with approximately 60,000 miles might be worth—then the hypothetical price might be eligible for some form of copyright protection in the right circumstances." *Id.* at 301. In the case at hand, Judge Karas wrote that "on a spectrum from fact to estimate suffused with judgment and opinion . . . , Plaintiff's data is legally equivalent to the unprotectable load ratings in *RBC Nice Bearings*, the likely unprotectable settlement prices in *New York Mercantile*, and the likely unprotectable analyst recommendations in *Barclays* . . . [and] unlike the protectable list of estimated prices of hypothetical used cars at issue in *Maclean Hunter*." *Id.* at 303. In so ruling, the court rejected the argument that the averages were estimates because they are not based on information from every single financial institution, noting that

> no white pages directory lists every single person living in a particular area, or gets every address, phone number, and name exactly right—indeed, the white pages at issue in *Feist* even contained four fictitious listings, inserted to detect copying—but that does not make the white pages a work of opinion regarding who lives in a given area. *See Feist*, 499 U.S. at 344. Likewise, in a case about the census that did not address copyright issues, the Supreme Court acknowledged that no population census can possibly capture everything about the population it surveys with complete accuracy. *See Dep't of Commerce v. U.S. House of Representatives*, 525 U.S. 316, 322 (1999) (describing the Census Bureau's methods for compensating for the "undercount," which is the portion of the population not directly surveyed either in person or by mail). And yet the Supreme Court stated in *Feist* that "[c]ensus data . . . do not trigger copyright" because "[c]ensus takers . . . do not 'create' the population figures that emerge from their efforts; in a sense, they copy these figures from the world around them." *Feist*, 499 U.S. at 347. So too here. Each average at issue in this case is a fact about the world—an "empirical reality"—even though it is in some sense an imperfect representation of some platonic ideal of a "national average bank rate."

978 F. Supp. 2d at 304. Judge Karas also rejected the argument that the fact that there were several competing companies that measured average rates, all of which regularly computed slightly different final values, meant that the output was anything other than "fundamentally factual in nature." *Id.* While different companies may consider different indicia relevant to consumers—such as, for example, the interest rate large banks pay on CDs with a $10,000 minimum deposit—"[t]hese differences do not undermine the conclusion that Plaintiff's data is fundamentally an attempt to represent an empirical fact about the world." *Id.* While plaintiff and its competitors used "slightly different inputs" to produce their "national average rate," "the level of judgment that goes into this decision is both minimal and, more relevant, of a type that does not render the output copyrightable. The differences in output come from the company's slightly different views about how best to represent empirical, historical

In a subsequent opinion in the case, Judge Karas held that a series of percentages of national interest rate averages were unprotectable as facts, tables of weekly averages of interest rates offered by banks were not copyrightable as compilations and the merger doctrine rendered plaintiff's list of national average rates of interest offered by banks for given financial products unprotectable under the Copyright Act.[32]

On the other hand, parts systems—even when elaborately compiled and highly complex—will not be deemed protectable where the parts numbers are factual and the catalogue or database is logical or functional, rather than reflecting creativity in the selection, arrangement, or organization of the parts.[33] Needless to say, a parts system that organizes like parts together will not be protectable, while one that is

---

reality, given time and resource constraints and the need to simplify reporting and analysis for some audiences." *Id.* at 305. Minimal judgment based on resource constraints, Judge Karas explained, does not merit copyright protection. *See id.*

With respect to the table of averages, the court held that plaintiff's list of averages, which was organized by date, lacked sufficient creativity in the selection and arrangement of the data to be protectable as a compilation. *See id.*

The court also held that even if plaintiff's averages were entitled to be treated as protected expression, the merger doctrine rendered them unprotectable. *See id.* at 308-12. Judge Karas explained that "the range of expression is not wide enough such that, if considered expressions, Plaintiff's averages would be distinct enough from their idea to prevent application of the merger doctrine . . . ." *Id.* at 310. Although average rates compiled by plaintiff and its competitors could vary by as much as 0.59 percentage points, "the crucial point is that their expressive variation is very low, even negligible, because the purpose of computing and publishing a national average rate is to give the consumer or the customer insight into the fact of what is going on in a national market." *Id.* at 310-11.

[32]*See BanxCorp v. Costco Wholesale Corp.*, 978 F. Supp. 2d 280, 292-312 (S.D.N.Y. 2013). BanxCorp's national interest rate averages were calculated using simple mathematical averages of reported rates from major banks, with no weighting or other calculations involved. *Id.* at 294. The output of the calculation was a single number that was "the exact mathematical average of the inputted rates as of a particular date." *Id.* at 298. The averages were called "benchmark rates" or "national average rates," were described as "current," "accurate," and "true," and were represented to consumers, customers, and the financial media. . . [as] objective facts about average national interest rates as of a particular date." *Id.* at 298-99. Additional details about the case and court's rulings may be found in the preceding footnote.

[33]*See, e.g., Southco, Inc. v. Kanebridge Corp.*, 258 F.3d 148, 152 (3d Cir. 2001) (denying a motion for preliminary injunction where the plaintiff

creative—for example, combining unrelated parts based on aesthetically pleasing arrangements or to form anagrams—would be unlikely to ever be copied because it would not be useful for its intended purpose (to organize and locate parts).

In other cases, courts have found used car valuations,[34] compiled property listings,[35] wholesale prices of used coins,[36]

---

sought to enjoin copying of a nine-digit part numbers assigned pursuant to an elaborate numbering system whereby each fastener was given a unique number, with each digit describing a specific physical parameter of the fastener, which the court held lacked the "modicum of creativity" required for copyright protection because a given number merely resulted from "the mechanical application of the numbering system."; although Southco had "devoted time, effort, and thought to the creation of the numbering system" the very existence of the system "made it impossible for the numbers themselves to be original."); *Southco, Inc. v. Kanebridge Corp.*, 390 F.3d 276 (3d Cir. 2004) (*en banc*) (reaffirming this principle and holding, in affirming summary judgment for the defendant, that copyright protection was not available because the parts numbers were rigidly dictated by the rules of the numbering system, and therefore not creative, and analogous to short phrases or titles of works, which lack sufficient creativity to be protectable); *R&B, Inc. v. Needa Parts Mfg. Inc.*, Copy. L. Rep. (CCH) ¶ 28,478 (3d Cir. 2002) (affirming the denial of plaintiff's motion for a preliminary injunction because plaintiff's parts numbers were dictated by its product classification scheme, and not the result of creativity); *R&B, Inc. v. Needa Parts Mfg., Inc.*, 418 F. Supp. 2d 684 (E.D. Pa. 2005) (accord) (granting defendant's motion for partial summary judgment); *ATC Distribution Group, Inc. v. Whatever It Takes Transmissions & Parts, Inc.*, 402 F.3d 700 (6th Cir. 2005) (holding that an automobile transmission parts catalog and the individual part numbers identified in the catalog were not copyrightable because (1) the part numbers were unprotectable due to merger and because the process of allocating numbers was not creative, and (2) the catalog did not qualify as a protectable compilation because the arrangement of the parts was based on a prior catalog and the parts were listed in a commonplace and practically inevitable manner).

[34]*See CCC Information Services, Inc. v. Maclean Hunter Market Reports, Inc.*, 44 F.3d 61, 67 (2d Cir. 1994) (holding the valuations protectable because they were original creations of Maclean Hunter "based not only on a multitude of data sources, but also on professional judgment and expertise.").

[35]*See Metropolitan Regional Information Systems, Inc. v. American Home Realty Network, Inc.*, 888 F. Supp. 2d 691 (D. Md. 2012) (entering a preliminary injunction based on the court's finding that the plaintiff was likely to prevail on its copyright infringement claim); *see also Metropolitan Regional Information Systems, Inc. v. American Home Realty Network, Inc.*, 904 F. Supp. 2d 530 (D. Md. 2012) (modifying the injunction and requiring the plaintiff to post a $10,000 bond).

[36]*See CDN Inc. v. Kapes*, 197 F.3d 1256, 1259-1261 (9th Cir. 1999) (holding wholesale prices contained in collectible coin guides protectable

Craigslist.org's compilation of user-submitted classified advertisements,[37] and healthcare ratings and awards given to

---

because, unlike the telephone listings at issue in Feist, which were simply provided by the phone company, CDN's coin valuations were "wholly creative"). As explained by the Ninth Circuit,

> CDN's process to arrive at wholesale prices begins with examining the major coin publications to find relevant retail price information. CDN then reviews this data to retain only that information it considers to be the most accurate and important. Prices for each grade of coin are determined with attention to whether the coin is graded by a professional service (and which one). CDN also reviews the online networks for the bid and ask prices posted by dealers. It extrapolates from the reported prices to arrive at estimates for prices for unreported coin types and grades. CDN also considers the impact of public auctions and private sales, and analyzes the effect of the economy and foreign policies on the price of coins. As the district court found, CDN does not republish data from another source or apply a set formula or rule to generate prices. The prices CDN creates are compilations of data that represent its best estimate of the value of the coins.

Id. at 1260. In so ruling, the panel was careful to explain the difference between protectable facts and protectable compilations of unprotectable facts:

> Appellant's attempt to equate the phone number listings in *Feist* with CDN's price lists does not withstand close scrutiny. First, Kapes conflates two separate arguments: (1) that the listing, selection, and inclusion of prices is not original enough to merit protection; and (2) that the prices themselves are not original creations. Whether CDN's selection and arrangement of the price lists is sufficiently original to merit protection is not at issue here. CDN does not allege that Kapes copied the entire lists, as the alleged infringer had in Feist. Rather, the issue in this case is whether the prices themselves are sufficiently original as compilations to sustain a copyright. Thus Kapes' argument that the selection is obvious or dictated by industry standards is irrelevant.

Id. at 1259; *see also National Football Scouting, Inc. v. Rang*, 912 F. Supp. 2d 985, 990 (W.D. Wash. 2012) (following *CDN* for the proposition that a "numeric expression of a professional opinion can be copyrightable" in holding that football player grades were copyrightable as a compilation of facts, but granting summary judgment for the defendant based on fair use).

Applying *CDN*, a district court held that even where numbers are protectable, copyright law does not extend to protect the fact that an entity won an award or ranked in the top tenth percentile based on the copyrighted ranking system. *Comparion Medical Analytics, Inc. v. Prime Healthcare Services, Inc.*, Case No. 2:14-CV-3448 SVW (MANx), 2015 WL 12746228, at *5-6 (C.D. Cal. Apr. 14, 2015).

CDN has been criticized to the extent it could be read to mean that the prices themselves were compilations. The price estimates may have involved originality and they may be elements of a compilation, "but they are not themselves compilations." *BanxCorp v. Costco Wholesale Corp.*, 978 F. Supp. 2d 280, 306 n.12 (S.D.N.Y. 2013), *quoting* James Grimmelmann, *Three Theories of Copyright in Ratings*, 14 Vand. J. Ent. & Tech. L. 851, 862 n.71 (2012).

[37] *See Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 971 (N.D. Cal. 2013). In *3Taps*, the court held that the database of user-submitted classi-

hospitals[38] entitled to copyright protection, while copyright protection was found unavailable for government building codes,[39] bearing load data,[40] a mathematical model based on

---

fied advertisements maintained at Craigslist.org was protectable where both the compilation and the individual advertisements were minimally creative, but that Craigslist could maintain suit for infringement only for a period of time during which it obtained an exclusive license from users to their classified advertisements, pursuant to its Terms of Use agreement, to which all users were required to assent.

[38]*See Health Grades, Inc. v. Robert Wood Johnson University Hosp., Inc.*, 634 F. Supp. 2d 1226, 1234 (D. Colo. 2009) (denying defendant's motion to dismiss where "Health Grades' healthcare ratings for RWJ and other medical providers are a product of Health Grades' collection of data and information from a variety of sources, which it then analyzes and weighs using its own proprietary methodologies to produce a Health Grades' rating of 1, 3 or 5 stars and/or awards for each healthcare provider reviewed. These ratings and awards are not, therefore, facts 'discovered' by Health Grades . . . , but rather are expressions . . . . These ratings only exist because Health Grades has selected, weighed and arranged facts it has discovered to present the collected data in a form . . . that can be used more effectively by the reader to make judgments about providers.").

In *Comparion Medical Analytics, Inc. v. Prime Healthcare Services, Inc.*, Case No. 2:14-CV-3448 SVW (MANx), 2015 WL 12746228, at *5-6 (C.D. Cal. Apr. 14, 2015), the court conceded that while a system of numeric grades for various hospitals may be protectable as a compilation of facts, an award based on those facts or a finding that an entity ranks in the top tenth percentile based on that ranking did not amount to copyrightable expression. In that case, a company that "grants to hospitals awards, and then sells them the right to publicize the awards . . ." sued a recipient of its awards for "posting news of the awards on its website . . ." without purchasing a proffered license to do so. In so ruling, the court distinguished *Robert Wood Johnson* as a case that focused on plaintiff's ratings.

[39]*See Veeck v. Southern Bldg. Code Congress Int'l, Inc.*, 293 F.3d 791, 802 (5th Cir. 2002) (*en banc*) (ruling in favor of a website operator who had pasted the text of model building codes on his site, and holding, subject to a strong dissenting opinion, that these codes were not protectable).

[40]*See RBC Nice Bearings, Inc. v. Peer Bearing Co.*, 676 F. Supp. 2d 9, 22 (D. Conn. 2009) (granting summary judgment for the defendant; "Although the state of the law regarding the copyrightability of numbers remains unclear, . . . the Court finds the bearing load data at issue in this case to be unprotectable facts . . . . [L]oad ratings are mainly a function of the geometry of the bearing and material . . . . [C]ertain other 'life factors' influence how load ratings are determined for a particular bearing, including tolerances, material cleanliness, lubrication, hardness, and operating temperature, and . . . these factors are enumerated in published industry guidelines . . . . [T]he bearing load ratings are essentially a numerical representation of the physical characteristics of a

the laws of physics,[41] "traffic conditions, speed restrictions and police-monitors" in the Waze crowd-sourced GPS and traffic app,[42] and average money market and certificate of

---

particular bearing . . . . While there may be some level of judgment involved in selecting which particular 'life factors' to utilize in adjusting the standard load rating calculation, . . . such judgment is very minimal given that the relevant life factors are published in industry guidelines.").

[41] *Ho v. Taflove*, 648 F.3d 489, 498-500 (7th Cir. 2011) (affirming summary judgment of non-infringement in favor of a defendant who copied plaintiffs' mathematical model applying a law of physics). As the court explained:

> The Model is an idea. In Professor Ho and Ms. Huang's own words, the Model "mimic[s] . . . certain behaviors of millions of particles in a photonic device." Appellants' Br. 4. That is, the Model attempts to represent and describe reality for scientific purposes. This scientific reality was not created by the plaintiffs. Rather, the Model embodies certain newly discovered scientific principles. Granted, as the plaintiffs note, the Model makes certain hypothetical assumptions, but those hypothetical assumptions do not render the Model fictitious. Rather, the Model strives to describe reality, and, as conceded at oral arguments, the value of the Model is its ability to accurately mimic nature. *See Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 9 F.3d 823, 842–43 (10th Cir. 1993) ("The constants in the Design Flex program represent scientific observations of physical relationships concerning the load that a particular belt can carry around certain sized gears at certain speeds given a number of other variables. These relationships are not invented or created; they already exist and are merely observed, discovered and recorded. Such a discovery does not give rise to copyright protection."). As the Supreme Court put it in *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 347, 111 S. Ct. 1282, 113 L. Ed.2d 358 (1991), "facts do not owe their origin to an act of authorship. The distinction is one between creation and discovery: The first person to find and report a particular fact has not created the fact; he or she has merely discovered its existence."

Id. at 498-99.

[42] *Phantomalert, Inc. v. Google Inc.*, No. 15-CV-03986-JCS, 2015 WL 8648669, at *10, 14 (N.D. Cal. Dec. 14, 2015) (dismissing plaintiff's copyright claim where the information that plaintiff alleged defendant copied was "inherently factual, involving 'traffic conditions, speed restrictions, and police-monitors,' that is, objective facts that can be discovered and reported . . . . "). *But see Phantomalert, Inc. v. Google Inc.*, No. 15-CV-03986-JCS, 2016 WL 879758, at *8-12 (N.D. Cal. Mar. 8, 2016) (granting defendants' motion to dismiss plaintiff's amended copyright infringement claim for failing to plausibly allege infringement but finding that, as amended, plaintiff plausibly alleged that "the location of some of the individual Points of Interest, as well as the[ir] overall arrangement . . . , are protectable (at least as a pleading matter)."). In its amended complaint, Phantomalert differentiated between actual driving conditions and "Points of Interest," alleging that Points of Interest were placed other than at the actual locations, based on judgments made about drivers' experience and what they would want to know, even if it related to hazards that did not directly affect them. *See id.* at *9. Phantomalert also alleged that its database used a system of categorization that the court found was characterized by some minimal degree of originality. *Id.* at *10. In fact,

deposit (CD) rates.[43]

While these determinations may be made on summary judgment[44] or at trial, there are an increasing number of copyrightability opinions decided in connection with motions to dismiss. Although a court may consider a claim to be *plausible,* which is what is required at the outset of a case when a court evaluates the allegations in connection with a motion to dismiss based on the pleadings, a more detailed analysis later in the case (based on evidence) may reveal a lack of originality in the selection, arrangement or organization of a factual compilation.

In contrast to facts or data, product descriptions, if sufficiently creative, may be entitled to copyright protection. In *MyWebGrocer, LLC v. Hometown Info, Inc.*,[45] the Second

---

the categories described (with the possible exception of "dangerous intersections" and "dangerous curves" which potentially might involve some creativity in what locations to include or exclude) appear to be entirely factual (railroad crossings, speed traps, speed cameras, potholes, school zones and red light cameras).

[43]*See BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 606 (S.D.N.Y. 2010).

[44]*See, e.g., NTE, LLC v. Kenny Construction Co.*, No. 14 C 9558, 2016 WL 1623290, at *4-6 (N.D. Ill. Apr. 25, 2016) (granting summary judgment for the defendant after finding that NTE's copyright extended to the "selection, arrangement and coordination" of data in the NTE system, including the particular way in which NTE's barcodes imbue the data with meaning, but that there was insufficient evidence that this (as opposed to unprotectable data) was copied).

Where summary judgment is sought, a plaintiff must clearly define what the alleged compilation is, where it is not clear from the face of a copyright registration what the work is. *See Cisco Systems Inc. v. Arista Networks, Inc.,* Case No. 14-cv-05344-BLF, 2016 WL 4440239, at *2-4 (N.D. Cal. Aug. 23, 2016) (denying the copyright holder's motion for summary judgment in a software copyright dispute in part because the plaintiff had not presented evidence of where its alleged compilation had come from or how and when it was compiled, in a case where the plaintiff did not own a single registration for the work but claimed infringement of a compilation composed of pieces drawn from 26 different copyright registrations covering Cisco's IOS, which the defendant characterized as "a lawyer created construct that simply mirrors. . . [the] copyright infringement allegations. . ." in plaintiff's Complaint). *See generally supra* § 4.07 (analyzing software copyright protection). In other circuits, but not the Ninth Circuit, a plaintiff generally would need to establish that a work was covered by a registration certificate in order to even state a claim. *See supra* § 4.08[2].

[45]*MyWebGrocer, LLC v. Hometown Info, Inc.*, 375 F.3d 190 (2d Cir. 2004).

Circuit affirmed the denial of a preliminary injunction in a case where the plaintiff had created 18,000 product descriptions for a grocery store chain whose website it maintained, which were copied verbatim by the new web host after the grocery store switched hosting services. The Second Circuit concluded that whether the product descriptions met the "minimum level of creativity" required for copyright protection was an issue to be decided on remand by the trial court. Among other things, the court emphasized that because the product descriptions differed from the ones used by the defendant on other grocery sites it hosted a "trier might conclude that MyWebGrocer made creative choices about what to include or exclude in its product descriptions," thus allowing for a finding of infringement. However, the court held that this outcome was not sufficiently likely to merit a preliminary injunction.[46]

On the other hand, in *Incredible Technologies, Inc. v. Virtual Technologies, Inc.*,[47] the Seventh Circuit affirmed a lower court finding that instructions for a videogame were not protectable or, if protectable, because the creativity was at most "slight" or "less than minimal," could only have been infringed by a showing of "identical copying." The appellate panel wrote that, "while there are arguably more ways than one to explain how the trackball system works, the expressions on the control panel . . . are utilitarian explanations of that system and are not sufficiently original or creative to merit copyright protection."[48]

Whether the contents of a database are separately protectable turns on the level of original, creative expression, as well as other factors analyzed in sections 4.02 and 4.07.

As noted above, where the selection,[49] arrangement or organization of otherwise unprotectable data (or preexisting

---

[46]*MyWebGrocer, LLC v. Hometown Info, Inc.*, 375 F.3d 190, 193–94 (2d Cir. 2004).

[47]*Incredible Technologies, Inc. v. Virtual Technologies, Inc.*, 400 F.3d 1007, 1013–14 (7th Cir. 2005).

[48]*Incredible Technologies, Inc. v. Virtual Technologies, Inc.*, 400 F.3d 1007, 1013 (7th Cir. 2005); *see also Allen v. Academic Games League of America, Inc.*, 89 F.3d 614, 617–18 (9th Cir. 1996) (applying the merger doctrine to deny protection to expression in game manuals).

[49]As a practical matter, the creativity inherent in the selection of articles or other more expressive works, if genuine selection or arrangement is involved, may be easier to establish than with purely factual data where the selection often serves logical or efficient purposes.

material owned by a third party, but not the database owner) reflect some minimal level of creativity, a database will be protectable as a compilation. A compilation will qualify for protection to the extent "selected, coordinated, or arranged in such a way that the resulting whole constitutes an original work of authorship."[50]

Where a database is all-inclusive it will not be entitled to copyright protection. "In order to obtain copyright protection, a compilation must be guided by principles of selection other than all-inclusiveness. This is because the collection of 'all is not a selection.' "[51] Thus, for example, in *Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*,[52] the Ninth Circuit held that Experian's list of compiled pairings of names and addresses in its Consumer View Database (CVD) was entitled to "limited protection."[53] Experian compiled its pairings from a variety of sources, such as catalogues, purchase data, cable company records, real estate deeds and warranty cards signed by consumers at retail stores. Experian excluded name and address pairings that it believed were not valuable to its clients, such as business addresses and addresses of individuals in prison and the very elderly. Experian also resolved conflicts between data sources, using thousands of "business rules" or algorithms to analyze data from each source and determine which name and address pairing should be included in CVD. Experian kept the data current and regularly updated its business rules. Experian estimated that it spent $10 million annually to compile and update the CVD.

In holding that Experian's pairings were entitled to limited copyright protection, the panel explained that "Experian's selection process in culling data from multiple sources and selecting the appropriate pairing of addresses with names

---

[50]17 U.S.C.A. § 101.

[51]*Silverstein v. Penguin Putnam, Inc.*, 522 F. Supp. 2d 579, 599 (S.D.N.Y. 2007), *quoting Silverstein v. Penguin Putnam, Inc.*, 368 F.3d 77, 85 (2d Cir.), *cert. denied*, 543 U.S. 1039 (2004). In *Silverstein*, the district court, on remand, held that a collection of poems was not entitled to copyright protection where essentially all poems by a given author were included in the work. There was thus no creativity in the selection made of what poems to include or exclude from the compilation.

[52]*Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176 (9th Cir. 2018).

[53]*Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176, 1185 (9th Cir. 2018).

before entering them in the database involves a process of at least minimal creativity. The listings are compiled by first collecting and comparing multiple sources, and then sorting conflicting information through the creation of business rules that Experian created to select from among the conflicts."[54]

Creativity in the selection and arrangement of otherwise unprotectable data, according to the Second Circuit, "is a function of (i) the total number of options available, (ii) external factors that limit the viability of certain options and render others non-creative, and (iii) prior uses that render certain selections 'garden variety.' "[55] Stated differently, "when it comes to the selection or arrangement of information, creativity inheres in making non-obvious choices from among more than a few options."[56] Thus, in *Feist Publica-*

---

[54]*Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176, 1185 (9th Cir. 2018).

[55]*Matthew Bender & Co. v. West Publishing Co.*, 158 F.3d 674, 682–83 (2d Cir. 1998), *cert. denied,* 526 U.S. 1154 (1999). This test was restated by Judge Preska to provide that a compilation may lack the requisite creativity where (1) industry conventions or other external factors dictate selection so that any person compiling facts of that type would necessarily select the same categories of information; (2) the author made obvious, garden-variety or routine selections; or (3) the author has a very limited number of options available. *O.P. Solutions Inc. v. Intellectual Property Network Ltd.,* No. 96 Civ. 7952 (LAP), 52 U.S.P.Q.2d 1818, 1823, 1999 WL 1122475 (S.D.N.Y. 1999).

[56]*Mathew Bender & Co. v. West Publishing Co.*, 158 F.3d 674, 682 (2d Cir. 1998), *cert. denied*, 526 U.S. 1154 (1999); *see also id.* at 689 (summarizing case law by noting that compilations were found protectable in cases where "the compiler selected from among numerous choices, exercising subjective judgment relating to taste and value that were not obvious and that were not dictated by industry convention."). By contrast:

> Selection from among two or three options, or of options that have been selected countless times before and have become typical, is insufficient. Protection of such choices would enable a copyright holder to monopolize widely used expression and upset the balance of copyright law.

Id. at 682.

One way to evaluate whether a compilation is protectable therefore "is to consider what . . . competitors would have to do to avoid an infringement claim." *Id.* In the context of the West Publishing Co. court reporters before it, the Second Circuit concluded that:

> West's claim illustrates the danger of setting too low a threshold for creativity or protecting selection when there are two or three realistic options: West lists only the arguing attorneys and city of practice, while United States Law Week lists the arguing and briefing attorneys, their firm affiliations and city and state of practice. If both of these arrangements were protected, publishers of judicial opinions would effectively be prevented from providing any useful ar-

tions, Inc. v. Rural Telephone Service Co.,[57] Justice O'Connor acknowledged that even a purely factual compilation of data, such as a phone book, could be entitled to copyright protection if it incorporated an original selection or arrangement.[58] The level of protection accorded a factual compilation, however, is "thin" because the underlying facts are unprotectable and what is "original" in the constitutional sense is merely the selection and arrangement.[59]

"All that is needed for a finding of sufficient originality is a 'distinguishable variation' that is not merely trivial, even if the copyrighted work is based on prior copyrighted or public domain works."[60] Thus, compilations assembled somewhat more creatively than the alphabetically arranged listing of all names, address and telephone numbers found in white page telephone directories have been held protectable.[61] By contrast, "insubstantial, unoriginal, and uncreative" compila-

---

rangement of attorney information for Supreme Court decisions that is not substantially similar to a copyrighted arrangement.

Id. at 684.

[57]*Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991).

[58]*Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 348 (1991).

[59]*Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 347-49 (1991).

[60]*Torah Soft Ltd. v. Drosnin*, 136 F. Supp. 2d 276, 286 (S.D.N.Y. 2001), *quoting Re-Alco Industries, Inc. v. National Center for Health Educ., Inc.*, 812 F. Supp. 387, 393 (S.D.N.Y. 1993) (citation omitted).

[61]*See, e.g., CCC Information Services, Inc. v. Maclean Hunter Market Reports, Inc.*, 44 F.3d 61 (2d Cir. 1994) (selection and arrangement of used automobile valuation criteria), *cert. denied*, 516 U.S. 817 (1995); *Key Publications, Inc. v. Chinatown Today Publishing Enterprises, Inc.*, 945 F.2d 509, 512–14 (2d Cir. 1991) (selection of particular businesses in specialized telephone directory for use by New York's Chinese-American community); *Kregos v. Associated Press*, 937 F.2d 700, 703–06 (2d Cir. 1991) (predictive pitching form based on selection of nine baseball statistics); *Harper House, Inc. v. Thomas Nelson, Inc.*, 889 F.2d 197, 204–05 (9th Cir. 1989) (selection and arrangement of materials in daily organizer); *BUC Int'l Corp. v. International Yacht Council Ltd.*, 489 F.3d 1129, 1145–51 (11th Cir. 2007) (affirming a jury finding that a factual compilation of yachts listed for sale by yacht brokers was entitled to copyright protection); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 972 (N.D. Cal. 2013) (holding that plaintiff plausibly stated a claim that classified listings, organized first geographically and then in categories of products or services, were protectable as a compilation); *Nielson Co. v. Truck Ads, LLC*, No. 08 C6466, 2011 WL 3857122, at *9-10 (N.D. Ill. Aug. 21, 2011) (finding that "Designated Market Area" maps that divide up television

tions have been held unprotectable.[62]

---

market areas with collected data about the programs viewed was copyrightable and not barred by the merger doctrine because estimation of viewership, unlike census data, is done through sampling and extrapolation and there are multiple ways to express DMA data); *Dataworks, LLC v. Commlog, LLC*, Civil Action No. 09-CV-00528-WJM-BNB, 2011 WL 2714087, at *5 (D. Colo. July 13, 2011) (finding that the "selection, design, and placement of the calendars, daily logs, repair and maintenance logs, collective repair lists . . ." in a blank log book used to record operational information were sufficiently original and creative to warrant copyright protection as compilations); *Madison River Management Co. v. Business Management Software Corp.*, 387 F. Supp. 2d 521, 534–35 (M.D.N.C. 2005) (holding protectable a database containing telephone customer information where the database imposed a new structure on raw data and included metadata enhancements); *O.P. Solutions, Inc. v. Intellectual Property Network Ltd.,* No. 96 Civ. 7952 (LAP), 52 U.S.P.Q.2d 1818, 1999 WL 1122475 (S.D.N.Y. 1999) (calendaring software for lawyers for PTO filings).

[62]*Matthew Bender & Co. v. West Publishing Co.*, 158 F.3d 674, 683 (2d Cir. 1998) (holding unprotectable the following elements of West Publishing Co.'s case reporters & CD-ROMs: captions, courts and date information; attorney listings; subsequent history; and parallel or alternative citations added by West), *cert. denied*, 526 U.S. 1154 (1999); *see also Victor Lalli Enterprises, Inc. v. Big Red Apple, Inc.*, 936 F.2d 671 (2d Cir. 1991) ("lucky numbers" used for gambling, generated by a formula that was standard in the industry); *Warren Publishing, Inc. v. Microdos Data Corp.*, 115 F.3d 1509 (11th Cir. 1997) (plaintiff "did not exercise any creativity or judgment in 'selecting' cable systems to include in its Factbook, but rather included the entire relevant universe known to it . . ."), *cert. denied*, 522 U.S. 963 (1997); *BellSouth Advertising & Publishing Corp. v. Donnelley Information Publishing, Inc.*, 999 F.2d 1436 (11th Cir. 1993) (*en banc*) (holding that categories for organizing material in a yellow pages telephone directory lacked creativity where many of the selected headings were deemed obvious (such as "attorneys" or "banks") and others resulted from standard industry practices), *cert. denied*, 510 U.S. 1101 (1994); *Torah Soft Ltd. v. Drosnin*, 136 F. Supp. 2d 276 (S.D.N.Y. 2001) (holding unprotectable a database version of the Hebrew Bible where the plaintiff's alterations were "nothing more than non-original changes dictated by the technological requirements of Bible code software and the end-user market"; where the replacement of final consonants of Hebrew letters with non-final consonants "required no skill beyond that of a high school . . . student and displayed no originality" and the substitution of various symbols involved "nothing more than a *de minimis* quantum of creativity" and the plaintiff "failed to demonstrate how an asterisk or a pound symbol is any more distinctive than a plus sign or an ampersand."; citations omitted); *Skinder-Strauss Associates v. Massachusetts Continuing Legal Educ., Inc.*, 914 F. Supp. 665, 676 (D. Mass. 1995) ("in compiling a Massachusetts directory of lawyers and judges, . . . the 'selection' of other directory data, including the attorney name, address, telephone and fax numbers, year of bar admission, and so forth are . . . unoriginal and determined by forces external to the compiler.").

A data compilation, such as a phone book, may be entitled to copyright protection, even though purely factual, if uniquely arranged in some artistic or creative manner, rather than alphabetically by last name or in some other logical manner.[63] A third party lawfully would be unable to make an exact duplicate of such an arguably creative compilation, although it would be permitted to copy factual information in the compilation and produce its own compilation (either in standard, alphabetical form, or in its own unique arrangement) so long as the amount copied (if the protectable feature of the database is the selection of its components) or the features reproduced or distributed in competition with the database (if it is the arrangement or organization of the data that is protectable) does not rise to the level of substantial similarity or virtual identicality.[64]

For online databases, creativity in the selection of incorporated facts is substantially more important than their arrangement. The arrangement of content in a database often is irrelevant (or merely functional—based on the most

---

[63]Needless to say, it is often the logical arrangement of data that makes a compilation most valuable to users, even though this feature may undermine entitlement to protection for the compilation under U.S. copyright law.

[64]Even an entire database potentially could be copied for internal analysis (as opposed to use in a competing database) if this form of intermediate copying was deemed a fair use because undertaken for a purpose that was permissible. *See Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1520–28 (9th Cir. 1992) (holding intermediate copying to make a noninfringing videogame interoperable a fair use); *Nautical Solutions Marketing, Inc. v. Boats.com*, 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121 (M.D. Fla. Apr. 1, 2004) (holding that "momentary copying of . . . public Web pages in order to extract yacht listings facts unprotected by copyright law constitutes a fair use . . . ."); *Ticketmaster Corp. v. Tickets.com, Inc.,* CV99-7654-HLH (VBKx), 2003 WL 21406289, at *5 (C.D. Cal. Mar. 7, 2003) ("Taking the temporary copy of the electronic information [from the Ticketmaster.com website database] for the limited purpose of extracting unprotected public facts leads to the conclusion that the temporary use of the electronic signals was 'fair use' and not actionable."); *see also Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003) (citing *Sega* and other cases for the proposition that intermediate copying is a fair use where the only effect of enjoining it would be to give the copyright owner control over noninfringing material produced by a competitor, which was stated in *dicta* as a warning to the plaintiff to not attempt to circumvent the court's order by reconfiguring its product to make it impossible for customers to extract data without making unauthorized copies); *see generally supra* § 4.10[1] (analyzing intermediate copying).

efficient way to store the data);[65] databases generally may be searched by users through multiple different means.[66] Factual databases therefore potentially may require greater creativity in selection to offset the lack of creative arrangement.

In addition to the selection and arrangements of underlying facts, their organization—such as the fields used in the structure of a database—may be entitled to limited copyright protection. Database fields may be protectable if their selection and organization is original and creative.[67] Aspects of the organization, selection or arrangement of a database driven by efficiency considerations, however, will be unprotectable.[68]

---

[65]Non-creative, efficient software routines are not protectable. *See supra* § 4.07.

[66]Databases typically are arranged in some logical (as opposed to creative) manner, to facilitate easy access by users. The arrangement of a database may be protectable if it is genuinely creative, rather than functional. As a practical matter, however, under the virtual identicality test, a plaintiff would only be able to protect a creatively arranged database if the identical arrangement were copied. *See infra* § 5.02[2]. It would not be difficult to rearrange the order of data in a database and create a copy that would be equally useful to a user as the original. Only if the creative selection of material were virtually identical would a rearranged, exact copy of the contents of a database be found infringing.

Even a creatively arranged factual compilation may be entitled to a lower level of protection when digitized because of the difficulty of translating the arrangement exactly from "hard copy" paper to bits and bytes. The arrangement used in a database may not mirror the arrangement used in a preexisting printed work. Hence, the creative aspect of the compilation (such as West Publishing Co.'s arrangement of court opinions) may be lost entirely when the work is digitized and stored in a database. *See Matthew Bender & Co. v. West Publishing Co.*, 158 F.3d 693, 702 (2d Cir. 1998) ("If one browses through plaintiffs' CD-ROM discs from beginning to end, using the computer software that reads and sorts it, the sequence of cases owes nothing to West's arrangement . . . . [A] copyrighted arrangement is not infringed by a CD-ROM disc if a machine can perceive the arrangement only after another person uses the machine to rearrange the material into the copyrightholder's arrangement."), *cert. denied,* 526 U.S. 1154 (1999).

[67]*See, e.g., Harbor Software, Inc. v. Applied Systems, Inc.*, 925 F. Supp. 1042, 1049 (S.D.N.Y. 1996).

[68]*See generally supra* § 4.07 (extensively analyzing efficiency limitations on copyright protection for software and databases). For example, a compilation "may lack the requisite creativity where: '(1) industry conventions or other external factors dictate selection so that any person compiling facts of that type would necessarily select the same categories of infor-

Copyright owners have long sought to protect their works by including deliberate errors in order to more easily detect acts of infringement. Copying false or inaccurate facts from a database, however, will not necessarily establish copyright infringement. In *Feist*,[69] for example, the defendant had copied an entire phone book—100% of plaintiff's work, including all false facts—but the Supreme Court nonetheless held for the defendant because copying unprotected elements does not amount to infringement. In assessing copyright infringement, false or inaccurate facts are treated like actual facts and are unprotectable because they lack sufficient originality.[70] By contrast, creative facts (or facts derived from a fictional work), unlike actual or false facts, may be protectable where the "creative facts" presented cumulatively amount to a derivative work copied from creative expression.[71]

---

mation; (2) the author made obvious garden-variety, or routine selections, or (3) the author has a very limited number of options available." *Silverstein v. Penguin Putnam, Inc.*, 522 F. Supp. 2d 579, 599 (S.D.N.Y. 2007) (quoting earlier cases); *see also Phantomalert, Inc. v. Google Inc.*, No. 15-CV-03986-JCS, 2015 WL 8648669, at *12 (N.D. Cal. Dec. 14, 2015) (quoting *Silverstein*).

[69]*Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 362 (1991).

[70]*See, e.g., Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 344 (1991) (seeded false facts, intended to detect copying); *Nester's Map & Guide Corp. v. Hagstrom Map Co.*, 796 F. Supp. 729, 733 (E.D.N.Y. 1992); *Skinder-Strauss Associates v. Massachusetts Continuing Legal Educ., Inc.*, 914 F. Supp. 665, 675 (D. Mass. 1995); *see also Phantomalert, Inc. v. Google Inc.*, No. 15-CV-03986-JCS, 2015 WL 8648669, at *7, 10 (N.D. Cal. Dec. 14, 2015) (elaborating that seeded, false and inaccurate facts are unprotectable under *Feist*); *BanxCorp v. Costco Wholesale Corp.*, 978 F. Supp. 2d 280, 304 (S.D.N.Y. 2013) (explaining that erroneous facts are unprotectable under *Feist*; "very often, data fails to be perfectly representative or entirely complete relative to what it is supposed to measure, but the data nevertheless remains fundamentally factual.").

False facts asserted as true may alternatively be treated as unprotectable facts under the infrequently cited *asserted truths doctrine*, because "it is the author's assertions within and concerning the work that the account contained in the book is truthful that trigger its application." *Corbello v. Valli*, 974 F.3d 965, 979 (9th Cir. 2020). The Ninth Circuit cautioned in *dicta*, however, that "that the asserted truths doctrine would not cover fictional works that use claims to truthfulness as a literary device, like the Orson Welles radio broadcast of 'War of the Worlds.' " *See id.* n.5, *citing Terror by Radio*, N.Y. Times, Nov. 1, 1938, at A22.

[71]*See Castle Rock Entertainment, Inc. v. Carol Publishing Group, Inc.*, 150 F.3d 132 (2d Cir. 1998) (holding defendants liable for copyright

If a database interface is novel, or allows for novel business uses, it may be entitled to patent protection.[72] Protection for the arrangement or interface of a database, or how it operates, under either patent or copyright law, would not extend to the underlying data.

5.02[2] Enforcement of Database Copyrights and the Virtual Identicality Standard

Where a database is comprised of copyrightable contributions such as company reports and analysis, copying even a tiny percentage of the database may be deemed copyright infringement if the parts taken are independently protectable and those aspects of the infringing product that were copied are at least substantially similar to that material.[1] The fact that part or all of a defendant's database or product is

---

infringement for creating the "SAT (Seinfeld Aptitude Test)", a trivia quiz book which tested readers' recollection of facts from the fictional television series "Seinfeld"; "unlike the facts in a phone book, which 'do not owe their origin to an act of authorship,' . . . each 'fact' tested by the SAT is in reality fictitious expression created by Seinfeld's authors . . . . [The] characters and events spring from the imagination of Seinfeld's authors").

[72]*See infra* § 8.04[3].

[Section 5.02[2]]

[1]*E.g.*, *Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 328–31 (S.D.N.Y. 2010) (entering a permanent injunction and awarding statutory damages, prejudgment interest and attorneys' fees (but only that portion of fees directly and predominantly concerned with the prosecution of plaintiffs' copyright claim, potentially reduced in light of the disparity in resources between the plaintiffs—major investments firms—and the defendant, and defendant's financial condition) in a case where the defendant was held liable for verbatim copying of 17 "sample" reports prior to the time it changed its practices in 2005), *rev'd on other grounds*, 650 F.3d 876 (2d Cir. 2011) (reversing judgment for plaintiffs on their claim for hot news misappropriation; the defendant did not appeal the copyright judgment); *see generally infra* § 5.04 (discussing the case in greater detail in connection with plaintiffs' common law misappropriation claim).

While reports, articles or other longer works that may be included in a database may contain sufficient original and creative content to be deemed protectable, and raw data or pure facts generally do not, in limited circumstances, as noted in section 5.02[1], "facts" or data may be accorded protection if sufficiently original and creative and not otherwise barred from protection by the merger doctrine. *See, e.g., Health Grades, Inc. v. Robert Wood Johnson University Hosp., Inc.*, 634 F. Supp. 2d 1226, 1232–38 (D. Colo. 2009) (denying defendant's motion to dismiss plaintiff's copyright infringement claim premised on the defendant hospital allegedly accessing plaintiff's website and assenting to its click-through license agreement more than 200 times and, in violation of the limited license,

*non*infringing will be irrelevant because infringement focuses on the portion copied, not the extent of material that may be genuine.[2]

On the other hand, if a database is comprised of material that independently is not entitled to copyright protection—such as unprotectable facts[3] or raw data—copying portions of the database is unlikely to be actionable under the Copyright Act. Although a factual database may contain the requisite level of creativity to be deemed protectable as a compilation, a copyright in a database could prove of limited value in protecting its constituent parts which, if unprotectable, may be freely copied unless the extent of copying is so great that the allegedly infringing portion is virtually identical (or at least substantially similar) to the portion that was copied. Where protectable, factual compilations generally are entitled to only "thin" protection[4] because it is the compilation, not its individual components, that is the protectable

---

commercially reproducing, modifying and/or distributing its healthcare provider award and ranking information from plaintiff's website in press releases and other marketing materials); *supra* § 5.02[1] (discussing the case in the context of copyrightability and the merger doctrine).

In *Robert Wood Johnson*, the defendant-hospital's own ranking information and awards presumably comprised a small fraction of the data in plaintiff's database.

Where the portion copied is protectable, a database owner may maintain a suit for infringement. As discussed below in the balance of section 5.02[2], where the portion copied is not independently protectable and copyright protection is premised on the selection, arrangement or organization of the database itself, suit may be maintained only where so much of the database has been copied that it is substantially similar or virtually identical to the original.

[2]*See, e.g.*, *Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1308 (11th Cir. 2020) ("adding new material to copied material doesn't negate (or even ameliorate) the copying."); *see generally supra* §§ 4.07, 4.08.

[3]*See supra* § 5.02[1] (discussing protectable and unprotectable facts).

[4]*See Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 349 (1991). As explained by the Supreme Court, "[n]otwithstanding a valid copyright, a subsequent compiler remains free to use the facts contained in an another's publication to aid in preparing a competing work, so long as the competing work does not feature the same selection and arrangement." *Id.* A copyright similarly may be accorded only thin protection where it builds on a particular style of a work. *See, e.g.*, *Zalewski v. Cicero Builder Dev., Inc.*, 754 F.3d 95, 106-07 (2d Cir. 2014) (characterizing as "very thin" a plaintiff's copyright in colonial home designs where the plaintiff made no attempt to distinguish those aspects of his designs that were original to him from those dictated by the form in which he worked; "Although he undoubtedly spent many hours on his designs, and

work. To prevail in litigation, many (but not all)[5] courts therefore have held that a plaintiff must show virtual identicality (or a heightened showing of similarity), rather than merely substantial similarity.[6] If an entire database

---

although there is certainly something of Plaintiff's own expression in his work, as long as Plaintiff adhered to a pre-existing style his original contribution was slight—his copyright very thin.").

[5]*See, e.g., BUC Int'l Corp. v. International Yacht Council Ltd.*, 489 F.3d 1129, 1145–51 (11th Cir. 2007) (affirming the district court's use of the substantial similarity test, rather than virtual identicality, in a case involving a factual compilation, because the case did not involve a claim of nonliteral infringement, but also noting that the defendant neglected to raise the potential applicability of the standard until trial—after it approved jury instructions based on the substantial similarity test—even though the Eleventh Circuit case that had approved of the virtual identicality standard had been on the books for many years).

[6]*E.g., Incredible Technologies, Inc. v. Virtual Technologies, Inc.*, 400 F.3d 1007, 1013 (7th Cir. 2005) (affirming the lower court's holding that documentation for a videogame was either unprotectable or not infringing because the creativity at most was "slight" absent a showing of "identical copying"); *Apple Computer, Inc. v. Microsoft Corp.*, 35 F.3d 1435, 1441–43 (9th Cir. 1994), *cert. denied*, 513 U.S. 1184 (1995); *TransWestern Publishing Co. LP v. Multimedia Marketing Associates, Inc.*, 133 F.3d 773, 776–77 (10th Cir. 1998) (compilation); *Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1302 n.6 (11th Cir. 2020) (explaining that while "virtual identicality" must be shown "[i]n special circumstances . . . ," it was inapplicable in that case; "Because the copying alleged here concerns source code, the substantial-similarity standard, rather than the heightened virtual-identicality standard, applies."); *MiTek Holdings, Inc. v. Arce Engineering Co.*, 89 F.3d 1548, 1558–59 n.24 (11th Cir. 1996) (holding that "virtual identicality" must be shown for a plaintiff to prevail on a claim of infringement of a compilation of nonliteral elements of a computer program; substantial similarity must be shown for other aspects of a work); *see also Matthew Bender & Co. v. West Publishing Co.*, 158 F.3d 693, 704–05 (2d Cir. 1998) (applying a heightened test for substantial similarity for factual compilations which required a showing of "very similar literal ordering or format" and/or extensive verbatim copying), *cert. denied,* 526 U.S. 1154 (1999).

Even where a court applies the traditional substantial similarity test, it may be difficult for a plaintiff to prevail in a suit for infringement of a database comprised of unprotectable elements entitled to protection based on the selection, arrangement or organization of the work, where less than the entire database is copied. *See, e.g., Ross, Brovins & Oehmke, P.C. v. Lexis Nexis Group*, 463 F.3d 478, 482–83 (6th Cir. 2006) (holding that although the developer's selection of legal forms in a compilation was sufficiently creative to warrant copyright protection, the selections made by the developer and software designer were not similar enough to be actionable where 61% of plaintiff's forms (or 350 out of 576) were used by the defendant; "First, Lexis did not include a sufficiently large percentage of the same forms to permit a finding of copying. Second, nonquantitative

has been copied, and the database is deemed protectable, the defendant may be held liable for infringement. Rarely, however, does a defendant blatantly copy an entire database that it offers to the public in competition with plaintiff's own work. More commonly, certain unprotectable facts are copied. For example, a database owner may review a competitor's database and extract those components not already in its own work. If a defendant merely copies portions of the database—such as unprotectable facts, public domain material or licensed articles—the defendant's acts of copying may not amount to infringement because of the limited amount copied and the fact that a "thin" copyright in a compilation will only protect the compilation as a whole.

At what point permissible copying of unprotectable facts from a protectable database rises to the level of infringement is difficult to pinpoint in the abstract, but the extent of copying must be substantial. Indeed, because a purely factual database is entitled to such a low level of protection, the extent of copying that must be shown before infringement will be found is much greater than when more creative works are plagiarized.

In *Experian Information Solutions, Inc. v. Nationwide*

---

aspects of the two compilations support the conclusion that Lexis created a new work rather than a copy of LawMode's.").

In *Expert Pages v. Buckalew*, No. C–97–2109–VRW, 1997 WL 488011 (N.D. Cal. Aug. 6, 1997), plaintiffs Expert Pages and Advice and Counsel Corp., which operated a website where litigation consultants advertised their services, sued a Virginia man who was alleged to have made a complete, unauthorized copy of plaintiff's website in order to be able to contact each of plaintiffs' advertisers by email to invite them to advertise on a competing site that he had established. The court granted the defendant's motion to dismiss for lack of personal jurisdiction in the interests of justice, based on the court's determination that it would have been unreasonably burdensome for the defendant—a young man—to litigate in California, when compared to the burden imposed on plaintiffs, which were companies owned by a practicing attorney. Although the court did not address the merits of plaintiffs' claim, it appears likely that they alleged verbatim copying of their website since they otherwise would have had difficulty challenging the defendant's act of copying the names and email addresses of individual advertisers. Whether a defendant's efforts to replicate a commercial database by systematically contacting each paying advertiser listed in it (or offering them free inclusion in the competing database) could constitute an unfair trade practice or common law misappropriation would likely depend on the effect of such competition on the original database, among other things.

Marketing Services Inc.,[7] the Ninth Circuit held that Experian's list of compiled pairings of names and addresses in its Consumer View Database (CVD) was entitled to "limited protection" based on "Experian's selection process in culling data from multiple sources and selecting the appropriate pairing of addresses with names before entering them in the database . . . ."[8] But the Ninth Circuit characterized the scope of protection for this factual work as "severely limited."[9] Applying the virtual identicality test, the panel held that a match rate of 80% with the defendant's database was "insufficient to establish a bodily appropriation of Experian's work."[10]

In *Assessment Technologies, LLC v. WIREdata, Inc.*,[11] Judge Posner of the Seventh Circuit held that a database comprised of 456 fields grouped into thirty-four separate tables contained sufficient creativity to be protectable,[12] but nonetheless ruled that the defendant was entitled to freely copy the data stored in the database from municipal governments (even though the plaintiff claimed that its copyright extended to this data) where the data had been collected and inputted by municipal tax assessors, not the plaintiff, and Wisconsin's open records law required that data be provided upon request unless entitled to copyright protection. Judge Posner wrote:

> [I]f WIREdata said to itself, "Market Drive is a nifty way of sorting real estate data and we want the municipalities to give us their data in the form in which it is organized in the

---

[7] *Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176 (9th Cir. 2018); *supra* § 5.02[1].

[8] *Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176, 1185 (9th Cir. 2018).

[9] *Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176, 1186 (9th Cir. 2018).

[10] *Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.*, 893 F.3d 1176, 1187 (9th Cir. 2018).

[11] *Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003).

[12] The court concluded that the "modest requirement [that the work involve sufficient originality to distinguish it from material in the public domain] is satisfied . . . because no other real estate assessment program arranges the data collected by the assessor in these 456 fields grouped into these thirty-four categories, and because the structure is not so obvious or inevitable as to lack the minimal originality required." *Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 643 (7th Cir. 2003).

> database, that is, sorted into AT's 456 fields grouped into its 34 tables," and the municipalities obliged, they would be infringing AT's copyright because they are not licensed to make copies of Market Drive for distribution to others; and WIREdata would be a contributory infringer (subject to a qualification concerning the fair-use defense . . .). But WIREdata doesn't want the compilation as structured by Market Drive . . . . It only wants the raw data, the data the assessors inputted into Market Drive.[13]

Judge Posner explained that, because the process of extracting the data did not involve making an unauthorized copy or a derivative work, the municipalities were free to do so.[14] He clarified that:

> It would be like a Westlaw licensee's copying the text of a federal judicial opinion that he found in the Westlaw opinion database and giving it to someone else. Westlaw's compilation of federal judicial opinions is copyrighted and copyrightable because it involves discretionary judgments regarding selection and arrangement. But the opinions themselves are in the public domain . . . and so Westlaw cannot prevent its licensees from copying the opinions themselves as distinct from the aspects of the database that are copyrighted.[15]

---

[13] *Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003).

[14] Judge Posner wrote in *dicta* that even if an unauthorized copy were made, it would almost certainly be a fair use intermediate copy. *See Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 644 (7th Cir. 2003), *citing Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1520–28 (9th Cir. 1992); *see generally supra* § 4.10[1] (analyzing intermediate copying as potentially but not always a fair use).

Judge Posner further warned that if the plaintiff tried to circumvent the decision by reconfiguring its database "in such a way that the municipalities would find it difficult or impossible to furnish the raw data to requesters . . . in any format other than that prescribed by [the plaintiff] . . . it might be guilty of copyright misuse." 350 F.3d at 645; *see generally infra* § 16.04[3] (analyzing copyright misuse). He further suggested that the plaintiff was "trying to use its copyright to sequester uncopyrightable data, presumably in the hope of extracting a licensing fee from WIREdata." 350 F.3d at 645.

[15] *Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 644 (7th Cir. 2003). This analogy may be imperfect because subscription databases typically restrict use by license, which may be permissible to the extent that the *quid pro quo* is access to a database. *See infra* § 5.03[1].

WIREdata is perhaps best understood as a case where, in the absence of privity of contract, a database owner could not restrict access to otherwise unprotectable data.

Similarly, in *Hutchins v. Zoll Medical Corp.*,[16] the Federal Circuit, applying First Circuit law, held that plaintiff's compilation copyright did not protect individual words and "fragmentary" phrases when removed from their form of presentation and compilation. The court explained that, "[a]lthough the compilation of public information may be subject to copyright in the form in which it is presented, the copyright does not bar use by others of the information in the compilation." In *Zoll*, the district court had found that the words and phrases on Mr. Hutchins' "Script and Word List" were standard CPR instructions devoid of "creative expression that somehow transcend the functional core of the directions . . . ."

In *American Massage Therapy Association v. Maxwell Petersen Associates, Inc.*,[17] a district court in Illinois held that a defendant could not be held liable for copying data from a database of massage therapists, even though the database possessed sufficient creativity to be deemed protectable because, in addition to name, address and telephone number, which were " 'entirely typical' of a directory, the listing of the membership category and type of therapist produces a sufficiently creative selection to make it original."[18] The court emphasized that copyright protection extends only to those components of a work that are original to the author and thus the defendant's copying of unprotectable facts did not amount to infringement. It wrote that "[p]laintiff may have been the first to discover and report the names and addresses but this data does not 'ow[e] its origin' to plaintiff."[19] Further, while the selection of data to be included in the database was original, the court found the arrangement and organization—listing names geographically—were not. Moreover, the fact that the plaintiff could have arranged the database in a different form that would have been creative did "not elevate the listing [i.e., the factual data] to the level

---

[16]*Hutchins v. Zoll Medical Corp.*, 492 F.3d 1377, 1383–84 (Fed. Cir. 2007).

[17]*American Massage Therapy Association v. Maxwell Petersen Associates, Inc.*, 209 F. Supp. 2d 941 (N.D. Ill. 2002).

[18]*American Massage Therapy Association v. Maxwell Petersen Associates, Inc.*, 209 F. Supp. 2d 941, 948 (N.D. Ill. 2002).

[19]*American Massage Therapy Association v. Maxwell Petersen Associates, Inc.*, 209 F. Supp. 2d 941, 947 (N.D. Ill. 2002), *quoting Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 361 (1991).

of creative."[20]

Database scraping cases also sometimes raise more traditional issues of software infringement. In *Compulife Software, Inc. v. Rutstein*,[21] for example, the court entered judgment for the defendants on plaintiffs' copyright infringement claim, holding that the percentage of HTML code copied incident to scraping plaintiff's database (which was used to generate insurance quotes) was quantitatively insignificant and the plaintiff had not met its burden of proving that it was qualitatively substantially similar. The court found that 282 lines of plaintiff's 347-line HTML source code program had been copied, but after filtering out unprotectable elements only 27 lines remained. Although plaintiff's copyright claim failed, the court entered judgment for the plaintiff on its trade secret misappropriation claim.[22]

In *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*,[23] the court denied the defendant's motion to dismiss, holding that Snap-on had presented sufficient evidence to show disputed facts on the issues of protection and infringement in a screen scraping case. In *Snap-on*, O'Neil, a competitor, repeatedly accessed Snap-On's database to copy data for Mitsubishi, a customer who was trying to transition from Snap-On's database hosting service to O'Neil, where the issue of whether Mitsubishi was authorized to allow O'Neil to access the database on its behalf was disputed.

The court found that Snap-on had presented evidence that it owned valid copyrights in its Net-Compass software, improvements to Mitsubishi's data and in the proprietary database used to run the software.

With respect to copying, Snap-On alleged that O'Neil's scraper program copied protectable elements of Snap-on's database, including the link structure and navigational element on the left-hand of the site. The court, however, denied summary judgment, finding that, among other things, what information had actually been copied was disputed by the parties.

---

[20]209 F. Supp. 2d at 949.

[21]*Compulife Software, Inc. v. Rutstein*, Case Nos. 9:16-CV-80808-REINHART, 9:16-CV-81942-REINHART, 2021 WL 3713173, at *13-18 (S.D. Fla. July 12, 2021).

[22]*See infra* § 5.09 (discussing that aspect of the case).

[23]*Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 683–86 (N.D. Ohio 2010).

Snap-on eventually obtained a general jury verdict, although it is not clear whether the verdict was based on Snap-On's claim for copyright infringement or for its other claims for trespass, breach of contract (based on its EULA), or violations of the Computer Fraud and Abuse Act.[24] The case is discussed in greater detail in section 5.05 in connection with Snap-On's trespass claim.

Where a database includes creative elements such as photographs (where the selection, arrangement and organization arguably involves greater creativity than with factual data) the database owner nonetheless may be powerless to prohibit copying if it does not own the copyrights to the individual components of the database that are copied, and the amount copied is less than the entire work. Indeed, a database owner may be unable to prevail in an infringement action if copying is undertaken for a fair use purpose (rather than to merely offer the same database to the public in competition with the database owner's product, which plainly would be infringing). For example, in *National Football Scouting, Inc. v. Rang*,[25] a district court in Washington found protectable grades assigned to different football players, but held that the use of a small number of these grades in connection with commentary and analysis was a fair use.

Intermediate copying of even an entire database may be deemed a fair use if undertaken for a lawful purpose such as extracting unprotectable data. In *Nautical Solutions Marketing, Inc. v. Boats.com*,[26] for example, the plaintiff sought and obtained a declaration that its copying of the defendant's database was a fair use. In that case, the defendant, *Boats.com*, owned and operated *Yachtworld.com*, a website that listed yachts available for sale. Each listing showed pictures with a description provided by the yacht broker who posted it. The descriptions used industry-standard headings

---

[24]*See Snap-On Business Solutions Inc. v. O'Neil & Associates, Inc.*, No. 5:09–CV–1547, 2010 WL 2650875 (N.D. July 2, Ohio 2010) (awarding costs but denying Snap-On's request for an award of attorneys' fees because under Ohio law contractual attorneys' fee provisions are unenforceable as contrary to public policy because they are viewed as encouraging litigation).

[25]*National Football Scouting, Inc. v. Rang*, 912 F. Supp. 2d 985, 991-95 (W.D. Wash. 2012) (entering summary judgment for the defendant).

[26]*Nautical Solutions Marketing, Inc. v. Boats.com,* No. 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121 (M.D. Fla. Apr. 1, 2004).

such as "electrical," "accommodations," "galley," and "sails and rigging." Yachtworld.com's listings had a distinctive look-and-feel: pictures of the yachts always appeared to the left of the description, the basic facts were shown in bullet-points, and a blue wave appeared on the left side of the screen.

Plaintiff Nautical Solutions operated a competing website, *Yachtbroker.com*. Nautical generated listings by using a spider program to make temporary copies of Boats.com's listings. Nautical extracted the descriptions and pictures from the temporary copies it created, discarded those copies, and then used the extracted information to create its own listings. Nautical also offered a "valet service" in which, with the yacht broker's permission, it copied descriptions and pictures from the broker's listings on other websites, such as *Yachtworld.com*, and pasted this information into *Yachtbroker.com*. Yachtbroker.com's appearance differed from that of *Yachtworld.com*: the pictures were to the right of the facts, the facts were in a table, and there was no blue wave shown.

Nautical sought a declaratory judgment of non-infringement after *Boats.com* accused Nautical of violating its copyright in the *Yachtworld.com* website. With regards to Nautical's valet service, the court noted that *Boats.com* did not hold the copyrights to the individual pictures and descriptions—the brokers who created the individual listings did.[27] *Boats.com* likewise was held not to be entitled to copyright protection for the organization of the descriptions

---

[27] *Nautical Solutions Marketing, Inc. v. Boats.com*, No. 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121, *1–2 & n.7 (M.D. Fla. Apr. 1, 2004). The copyright owners of the individual photos included in the Boats.com database potentially could have maintained claims for infringement of their separate copyrights in their individual photos, if they had wanted to do so. As a practical matter, however, these copyright owners would have been unlikely to want to sue because their photos were most likely placed online to generate interest in the properties and potential sales. Wider distribution of the photos would likely serve their commercial interests. Given the purpose for which the photos were taken (to sell the properties featured in the photos), it is also unlikely that the individual copyright owners registered their copyrights prior to placing them online, and thus it is unlikely that they could have recovered statutory damages for infringement (and actual damages or wrongful profits potentially would have been *de minimis*). *See supra* §§ 4.08[2], 4.13. In addition, because the yacht owners had given permission to Nautical Solutions to copy their Boats.com listings, Nautical potentially would have been able to assert an implied license defense if the individual

because its use of industry-standard headings lacked creativity. Further, while Boats.com's copyright did extend to the website's distinctive look-and-feel, Nautical's website had its own unique look-and-feel and had not copied Boat.com's.[28]

The court held that Nautical's copying of *Boats.com* broker listings using a spider program called "Boat Rover" constituted a fair use.[29] Unlike the valet service, the spider program copied the entire website, including its protected look-and-feel. The court nonetheless deemed this allowable intermediate copying because the spider program only extracted unprotected facts from the copied site.[30] The court found no evidence of harm to the "potential market value for or value of Yachtworld.com," and stressed that the "amount and substantiality of the portion used" was minimal, since Nautical's final product was free of infringing material.[31]

Fair use also was influential in *NTE, LLC v. Kenny Construction Co.*,[32] an unreported opinion in which the court granted summary judgment for the defendant on a copyright infringement claim based on the defendant's having accessed plaintiff's database to extract its own raw data. Citing *As-*

---

brokers had then turned around and sued Nautical (although permission from individual brokers would not have supported an implied license to copy the compilation, in which Boats.com, not the individual owners, owned the relevant copyright). *See supra* §§ 4.05[7] (implied license), 5.01 (split copyrights in compilations).

[28]*Nautical Solutions Marketing, Inc. v. Boats.com*, No. 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121, at *3 (M.D. Fla. Apr. 1, 2004).

[29]*Nautical Solutions Marketing, Inc. v. Boats.com*, No. 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121, at *2 (M.D. Fla. Apr. 1, 2004).

[30]*See Nautical Solutions Marketing, Inc. v. Boats.com*, No. 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121, at *3 (M.D. Fla. Apr. 1, 2004) ("Boat Rover's momentary copying of Yachtworld's public web pages in order to extract from yacht listings facts unprotected by copyright law constitutes a fair use and thus " 'is not an infringement of copyright.' ") (citation omitted).

[31]*Nautical Solutions Marketing, Inc. v. Boats.com*, No. 8:02–CV–760–T–23TGW, Copy. L. Rep. (CCH) P28,815, 2004 WL 783121, at *2 & n.10 (M.D. Fla. Apr. 1, 2004).

[32]*NTE, LLC v. Kenny Construction Co.*, No. 14 C 9558, 2016 WL 1623290, at *5 (N.D. Ill. Apr. 25, 2016).

sessment Technologies, LLC v. WIREdata, Inc.[33] for the proposition that it could constitute "copyright misuse" to prevent a company from using its own data, and *Sega Enterprises Ltd. v. Accolade, Inc*.[34] on fair use intermediate copying, the court explained that in *NTE*, "after extracting the NTE reports, Kenny ended up in possession only of data that it undeniably owns or is in the public domain, which is to say the facts pertaining to the location of Kenny's materials across time. The contested data was input into the NTE system by Kenny in the first place and does not cease to belong to Kenny just because it is manipulated by a copyrighted software system."[35]

Because fair use is determined by a multipart balancing test which focuses on factors such as the degree of transformativeness and the use's impact on the value of or potential market for the copyright owner's work,[36] not all intermediate copying will necessarily be treated the same way deemed fair. Only intermediate copying undertaken for a lawful purpose will be deemed permissible. Because fair use is not determined by a bright line test, companies or individuals who build business models based on fair use may nonetheless get sued for infringement (as well as any other claims that might be brought).[37]

5.03 Contractual and Licensing Restrictions

5.03[1] In General

Owners of commercial databases generally seek to protect their rights through end-user license agreements (EULA), database access, use or subscription agreements or similarly-termed contracts or licenses.[1] These agreements typically may include terms prohibiting commercial use, the use of

---

[33] *Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 646-47 (7th Cir. 2003).

[34] *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1520–28 (9th Cir. 1992).

[35] *NTE, LLC v. Kenny Construction Co.*, No. 14 C 9558, 2016 WL 1623290, at *5 (N.D. Ill. Apr. 25, 2016).

[36] *See supra* § 4.10[1].

[37] *See infra* §§ 5.03 to 5.09, 5.11.

[Section 5.03[1]]

[1] The difference between an intellectual property license and a mere contract is addressed in chapters 14 and 16.

bots or other automated means to access a site or extract data, repeated access to a database, reverse engineering and unauthorized use or access, among other provisions, in addition to disclaiming liability and otherwise generally establishing the terms and conditions of use.[2] Whether and to what extent these purported use restrictions are effective depends on whether a binding contract has been formed, whether the agreement is part of a broader intellectual property license or merely a stand-alone data contract, whether the agreement is deemed enforceable, and the express or implied rights and restrictions set forth in it. Contract claims generally will not be preempted by the Copyright Act where an additional element (beyond mere copying)—such as the contractual obligation itself—has been alleged.[3]

---

[2]*See infra* chapter 22 (discussing Terms of Use for database and other sites and services).

[3]*See, e.g., ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1452–53 (7th Cir. 1996) (holding the plaintiff's breach of contract claim based on a shrinkwrap license for a CD containing phone directly listings not preempted); *BanxCorp v. Costco Wholesale Corp.*, 978 F. Supp. 2d 280, 315-16 (S.D.N.Y. 2013) (holding that plaintiff's claim for breach of contract was not preempted); *BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 611–18 (S.D.N.Y. 2010) (holding that claims for breach of a license agreement and misappropriation based on hot news were not preempted in a case alleging that the defendant, a licensee, misused money market and CD data, but claims for unfair competition and unjust enrichment were preempted); *Health Grades, Inc. v. Robert Wood Johnson University Hosp., Inc.*, 634 F. Supp. 2d 1226, 1242–47 (D. Colo. 2009) (holding plaintiff's claim that the defendant hospital breached its click-through license agreement with the plaintiff by commercially reproducing, modifying and/or distributing its healthcare provider award and ranking information from plaintiff's website in press releases and other marketing materials was preempted, but that its breach of contract claim based on unauthorized use of the plaintiff's mark in a way that implied that the owner endorsed the hospital's services was not preempted); *Internet Archive v. Shell*, 505 F. Supp. 2d 755, 763–64 (D. Colo. 2007) (holding that breach of contract and conversion claims arising out of a site owner's objection to her site being copied for inclusion in the Internet Archive's Wayback machine were not preempted); *Huckshold v. HSSL, LLC*, 344 F. Supp. 2d 1203 (E.D. Mo. 2004) (holding trade secret misappropriation and breach of contract claims not preempted where the plaintiff alleged that the defendant owed a duty to protect the confidentiality of plaintiffs' trade secrets and breached its contract by allowing a third party to copy the software in violation of their agreement (and not merely that the defendant itself copied the software), which thus involved an extra element, but finding plaintiff's tortious interference claim preempted where the only element needed to be shown to establish liability was copying); *see generally supra* § 4.18[1] (analyzing copyright preemption).

Where parties negotiate the terms of a database access agreement or where a written or electronic signature is obtained on a contract,[4] formation issues do not arise. However, where access to or use of a database is conditioned on a EULA or Terms posted on a website and accessed from a computer or mobile phone, whether the terms are deemed to form a binding contract in practice may depend on whether they are presented as a click-to-accept contract or otherwise structured so that express assent is obtained (or, at a minimum, that users were provided with reasonable notice and manifested assent).[5]

---

[4]*See infra* § 15.02 (electronic signatures).

[5]*See, e.g.*, *Emmanuel v. Handy Technologies, Inc.*, 992 F.3d 1, 8-10 (1st Cir. 2021) (affirming the district court's order enforcing Terms of Service in a mobile app under Massachusetts law, and compelling arbitration, where "Emmanuel had reasonable notice of the mandatory arbitration provision in the Agreement that Handy seeks to enforce when she selected 'Accept' on that app at that time, such that . . . she was bound by it."); *Meyer v. Uber Technologies, Inc.*, 868 F.3d 66 (2d Cir. 2017) (enforcing an online arbitration agreement where the company provided reasonable notice of the terms and the consumer manifested assent); *Dohrmann v. Intuit, Inc.*, 823 F. App'x 482, 484-85 (9th Cir. 2020) (reversing the lower court's denial of Intuit's motion to compel arbitration, where, to access a TurboTax account during the relevant time period, a user, after entering a user ID and password, was required to click a "Sign in" button, directly under which appeared the text "By clicking Sign In, you agree to the Turbo Terms of Use, TurboTax Terms of Use, and have read and acknowledged our Privacy Statement," which the majority deemed to provide conspicuous notice, over the dissent's objection that, among other things, the appearance of links to two different products' terms of use on the sign-in screen, Turbo Terms of Use and TurboTax Terms of Use, was confusing); *Lee v. Ticketmaster L.L.C.,* 817 F. App'x 393, 394-95 (9th Cir. 2020) (affirming the lower court's order compelling arbitration, holding that "Lee validly assented to Ticketmaster's Terms of Use, including the arbitration provision, each time he clicked the 'Sign In' button when signing into his Ticketmaster account, where three lines below the button, the website displayed the phrase, 'By continuing past this page, you agree to our Terms of Use,' as well as each time he clicked the 'Place Order' button when placing an order for tickets, where directly above the button, the website displayed the phrase, 'By clicking "Place Order," you agree to our Terms of Use,' where in both contexts, '"Terms of Use" was displayed in blue font and contained a hyperlink to Ticketmaster's Terms."); *Hancock v. AT&T Co.*, 701 F.3d 1248, 1256-58 (10th Cir. 2012) (affirming dismissal based on enforceable forum selection and arbitration provisions in an agreement that consumers were required to accept by clicking on an "I Acknowledge" button on a website presented to the user on a technician's laptop prior to installation, where "basic contract law principles in Florida and Oklahoma indicate that if a clickwrap agreement gives a consumer reasonable notice of its terms and the consumer affirmatively manifests

To be enforceable, a user must assent to a database license or contract, either expressly or impliedly based on notice and subsequent conduct (in using the database).[6] As analyzed extensively in section 21.03, unilateral online contracts are much more likely to be found binding where express assent is obtained, such as through a click-through contract (even though theoretically, a contract should be equally enforceable where it is formed based on implied assent such as conduct in the face of actual or imputed notice). While posted Terms of Use may be enforced where a defendant acknowledges that it had actual knowledge of the terms and proceeded to access a database or site thereafter or was repeatedly notified of the terms,[7] implied assent is more dif-

---

its assent to the terms, the consumer is bound by the terms."); *Kauders v. Uber Technologies, Inc*., 486 Mass. 557, 159 N.E.3d 1033 (2021) (requiring reasonable notice and a manifestation of assent); *see generally infra* § 21.03[2] (analyzing the issue more extensively and citing additional cases).

Case law and strategies for maximizing the potential enforceability of a unilateral agreement online are set forth in chapters 21 and 22, including sections 21.03 (online and mobile contract formation) and 21.04 (unconscionability).

[6]Contract formation for unilateral Internet contracts is addressed extensively in chapters 21 and 22. While cases involving databases are discussed in this section, exclusive consideration of database formation case law could lead to a skewed view of the state of the law of contract formation generally. Readers are encouraged to review chapters 21 and 22 in drafting, evaluating or litigating database agreements.

[7]*See, e.g., Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004) (holding that the district court was within its discretion in finding that the plaintiff was likely to prevail on the merits for purposes of granting a preliminary injunction where the defendant received actual notice of purported restrictions on access to a database but continued to repeatedly access the database on a daily basis even after receiving notice); *Gutierrez v. FriendFinder Networks Inc.*, Case No. 18-cv-05918-BLF, 2019 WL 1974900, at *7-8 (N.D. Cal. May 3, 2019) (enforcing the Terms of Use of an adult website, and compelling arbitration, where a recording of a call with plaintiff established that he was told by Customer Service, in connection with restoring access to the site in 2013 after being suspended for a Terms of Use violation, that he was required to adhere to the Terms, which he acknowledged he knew was required; "Because the Terms clearly stated that continued use of the site would constitute acceptance of the Terms, Plaintiff's continued use of the site after being put on notice of the Terms and his need to comply with them constituted acceptance of the Terms."); *Andra Group, LP v. BareWeb, Inc.*, Civil Action No. 4:17-CV-00815, 2018 WL 2848985, at *9 (E.D. Tex. June 11, 2018) (denying BareWeb's motion to dismiss Andra's breach of contract claim alleging that the competing online lingerie website copied tips it provided on its HerRoom.com website

ficult to prove in court absent this type of admission. Where Terms merely have been posted online and the defendant disputes knowing that it was bound by those terms, courts will be reluctant to find that a binding contract has been formed absent evidence that reasonable notice was provided to the user, which typically requires more than merely posting the Terms on a website or in a mobile app (and the Ninth

---

for consumers in violation of HerRoom.com's browsewrap agreement, where the court found that Andra alleged a plausible claim that was not preempted by the Copyright Act because (1) BareWeb's employees accessed HerRoom and (2) BareWeb's website used "terms of use similar to [Andra's] Terms of Use" and "publishe[d] the link to its website terms of use on its home page, in a similar location to where [Andra] publishe[d] a link to [Andra's TOU Agreement]" and therefore, because it used a similar agreement on its own website, BareWeb knew or should have known about the browsewrap agreement); *DHI Group, Inc. v. Kent*, Civil Action H–16–1670, 2017 WL 4837730, at *2-4 (S.D. Tex. Oct. 26, 2017) (denying DHI's motion to dismiss Oilpro's breach of contract claim where Oilpro alleged that DHI had actual knowledge of Oilpro's browsewrap agreement and nonetheless scraped OilPro's website in violation of those contractual terms); *Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007) (holding that the defendant was bound by posted Terms that formed a non-exclusive license to access Ticketmaster's website where the defendant acknowledged that it was on notice that its access to the site was subject to Terms); *Southwest Airlines Co. v. BoardFirst, LLC,* No. 3:06-cv-0891-B, 2007 WL 4823761 (N.D. Tex. Sept. 12, 2007) (holding that the defendant, operator of a site that offered a service to enhance Southwest Airline's passengers' ability to obtain a boarding pass with a high boarding priority level, had knowledge of and therefore was bound by Southwest's website Terms and Conditions of Use which prohibited third parties from accessing user accounts for commercial use, at least as of the time it was sent a cease and desist letter); *Cairo, Inc. v. Crossmedia Services, Inc.*, No. C 04-04825 JW, 2005 WL 756610 (N.D. Cal. Apr. 1, 2005) (following *Register.com* in holding that repeated use of a website with actual knowledge of the posted Terms of Use effectively binds a party to those terms); *Ticketmaster Corp. v. Tickets.com, Inc.,* CV99-7654-HLH (VBKx), 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003) (finding a triable issue of fact precluding summary judgment on the issue of whether the defendant was bound by posted Terms of Use where express assent was not obtained but the defendant had been put on written notice of the conditions governing use of the internal pages of plaintiff's website and thereafter continued to access them); *see also, e.g.*, *Southwest Airlines Co. v. Roundpipe, LLC*, 375 F. Supp. 3d 687, 706 (N.D. Tex. 2019) (denying defendant's motion to dismiss where the plaintiff alleged that defendants used automated scraping tools to access Southwest's website in violation of the terms and conditions of Southwest's website use agreement, where the defendant did not specifically challenge the contract formation process but instead argued that it was entitled to rely on contractual estoppel, which the court deemed premature for consideration in connection with a motion to dismiss); *see generally infra* § 21.03.

Circuit has further held that merely posting Terms on a website (even where accessible via a link from every page on the site), or in a mobile app, is insufficient to form a contract as a matter of law).[8]

---

[8]*See, e.g., Cullinane v. Uber Technologies, Inc.*, 893 F.3d 53, 60-64 (1st Cir. 2018) (reversing the lower court's order compelling arbitration based on the finding that the notice of terms presented to consumers was not reasonably conspicuous under Massachusetts law where Uber's "Terms of Service & Privacy Policy" hyperlink "did not have the common appearance of a hyperlink" because it was not "blue and underlined" but instead was presented in a gray rectangular box in white bold text, and where the content on the "Link Screen" and "Link Payment" screens contained other terms displayed with similar features, which diminished the conspicuousness of the "Terms of Service & Privacy Policy link and notice, in the view of the appellate court); *Starke v. Squaretrade, Inc.*, 913 F.3d 279, 292-97 (2d Cir. 2019) (holding an arbitration provision in post-transaction Terms & Conditions unenforceable because the plaintiff was not provided with reasonable notice); *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220 (2d Cir. 2016) (reversing the lower court's order dismissing plaintiff's complaint, holding that whether the plaintiff was on inquiry notice of contract terms, including an arbitration clause, presented a question of fact where the user was not required to specifically manifest assent to the additional terms by clicking "I agree" and where the hyperlink to contract terms was not "conspicuous in light of the whole webpage."); *Specht v. Netscape Communications Corp.*, 306 F.3d 17, 22–24 (2d Cir. 2002) (declining to enforce an arbitration provision and finding assent lacking where users of Netscape's website were urged to download free software by clicking on a button labeled "Download" but would not even have seen an invitation to review the license agreement available by hyperlink unless they scrolled down to the following page, where the full terms, which warned users that they should not download the software if they did not agree to be bound and included the arbitration provision, were only accessible via that link, and where the defendants alleged that they in fact were unaware that the free software was provided subject to terms); *Sgouros v. TransUnion Corp.*, 817 F.3d 1029, 1033-36 (7th Cir. 2016) (affirming denial of defendant's motion to compel arbitration where users were presented with a button and the words "I Accept & Continue to Step 3" but the "block of bold text below the scroll box told the user that clicking on the box constituted his authorization for TransUnion to obtain his personal information. It sa[id] nothing about contractual terms. No reasonable person would think that hidden within that disclosure was also the message that the same click constituted acceptance of the Service Agreement."); *Wilson v. Huuuge, Inc.*, 944 F.3d 1212 (9th Cir. 2019) (affirming the denial of defendant's motion to compel arbitration where its Terms of Use, which contained the arbitration provision, were accessible from settings in the defendant's mobile app); *McGhee v. North American Bancard, LLC*, 775 F. App'x 718 (9th Cir. 2019) (affirming denial of defendant's motion to compel arbitration where the link to the user agreement, on defendant's Terms and Conditions webpage, did not require any affirmative action to demonstrate assent and simply contained the invitation to "View the User Agreement

Indeed, courts frequently are hostile to efforts to enforce unilateral online agreements in the absence of express assent.[9] The absence of a binding contract could be especially problematic for database owners and website licensors whose agreements purport to restrict use of factual data (as opposed to reports, articles or other creative content entitled to copyright protection, independent of the database compilation).[10]

Courts increasingly use a lexicon of assorted jargon to refer to the various ways in which a contract may be formed online, including *clickwrap* and *browsewrap* agreements, and hybrids characterized by Eastern District of New York Judge Jack Weinstein as so-called *scrollwrap*[11] and *sign-in-*

---

here"); *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1175-79 (9th Cir. 2014) (declining to enforce an arbitration clause contained in website Terms of Use where there was no evidence that the website user had actual knowledge of the agreement, despite the fact that the Terms were accessible via a link from the bottom of every single page of the website, finding no contract as a matter of law); *Alan Ross Machinery Corp. v. Machinio Corp.*, No. 17-cv-3569, 2018 WL 3344364, at *5-6 (N.D. Ill. July 9, 2018) (dismissing Alan Ross Machinery's breach of contract claim, in a case alleging that Machinio scraped sales listings of industrial machinery from Alan Ross's website and duplicated those listings on its website in violation of its Terms and Conditions, where the T&Cs were merely posted on Alan Ross's website and made accessible via a link from every page on the website because "hyperlinking the terms and conditions at the bottom of every page is insufficient to provide adequate constructive notice" and, to establish express knowledge, "it is not enough to allege that Machinio was told not to scrape the website. Instead, Alan Ross must allege that Machinio had knowledge of the terms and conditions."); *A.V. v. iParadigms, LLC*, 544 F. Supp. 2d 473, 485 (E.D. Va. 2008) (declining to enforce an indemnification provision contained in defendant's Usage Policy, which was accessible via a link from every page on the website, where there was no evidence to impute knowledge of the terms to the plaintiffs and where the clickwrap agreement for the site, which unlike the Usage Policy was held enforceable, did not incorporate the Policy by reference and included an integration clause that stated that the clickwrap agreement "constitutes the entire agreement . . . with respect to usage of this Website."), *aff'd in part and rev'd in part on other grounds*, 562 F.3d 630, 639 (4th Cir. 2009); *see generally infra* § 21.03 (analyzing case law and the circumstances under which courts will enforce unilateral contracts based on implied assent).

[9] *See infra* § 21.03.

[10] *See supra* § 5.02.

[11] A *scrollwrap* agreement, using Judge Weinstein's terminology, requires a user to scroll through the terms before the user can assent to the contract by clicking on an "I agree" button. *See Berkson v. Gogo LLC*,

wrap agreements.[12] This jargon may obscure, rather than clarify the question of whether express or implied assent was obtained.

While the ever increasing number of cases evaluating various means for obtaining online assent are analyzed extensively in section 21.03, the bottom line for database owners

---

97 F. Supp. 3d 359, 386, 398-99 (E.D.N.Y. 2015). Judge Weinstein would put in this category cases typically categorized as *clickwrap* or express assent opinions such as *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229, 236–38 (E.D. Pa. 2007) (enforcing Google's AdWords clickwrap contract where there was reasonable notice of and mutual assent to the agreement; the contract was immediately visible in a scrollable text box below a prominent admonition in boldface to read the terms and conditions carefully and only assent if the user agreed to the terms, the terms were presented in twelve-point font and was only seven paragraphs long and was available in a printer-friendly, full-screen version; according to Judge Weinstein, "the plaintiff had the duty to read terms that were presented in a scroll box and required a click to agree and, therefore, the fact that the entire contract was not visible in the scroll box was irrelevant"); *Bar–Ayal v. Time Warner Cable Inc.*, No. 03–CV–9905, 2006 WL 2990032, at *9–10 (S.D.N.Y. Oct. 16, 2006) (finding acceptance where scrolling though thirty-eight screens of text was required—essentially the entire agreement); *Moore v. Microsoft Corp.*, 293 A.D.2d 587, 741 N.Y.S.2d 91, 92 (2d Dep't 2002) (holding that a contract was formed when "[t]he terms of the [agreement] were prominently displayed on the program user's computer screen before the software could be installed," and "the program's user was required to indicate assent to the [agreement] by clicking on the 'I agree' icon before proceeding with the download"); *In re RealNetworks, Inc.*, No. 00–CV–1366, 2000 WL 631341, at *6 (N.D. Ill. May 8, 2000) (approving a license agreement placed in a pop-up window with scroll bar).

[12] *See Berkson v. Gogo LLC*, 97 F. Supp. 3d 359, 392-402 (E.D.N.Y. 2015). A *sign-in-wrap* agreement notifies a user of the existence of terms of use but instead of providing an "I agree" button, advises the user that he or she is agreeing to the terms when registering or signing up for the site or service. *See id.* at 399-400. Judge Weinstein would put in this category *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829 (S.D.N.Y. 2012), where express assent was found but the court characterized the agreement as a 'hybrid." Judge Weinstein, analyzing self-described hybrid cases which he characterized as involving so-called sign-in-wrap agreements, explained that these type of agreements have been enforced based on "notice and an effective opportunity to access terms and conditions" in cases where (1) there is a hyperlink to the Terms next to the only button that will allow a user to continue use of the website, (2) the user registered or signed up for a service "with a clickwrap agreement and was presented with hyperlinks" to the Terms; or (3) notice of hyperlinked terms "is present on multiple successive webpages of the site." *Berkson v. Gogo LLC*, 97 F. Supp. 3d at 401.

As analyzed in section 21.03, these fine distinctions based on past district court cases are not really helpful in evaluating express or implied assent. *See infra* § 21.03.

is that it is always safer to obtain express assent to a database access agreement or EULA—and failing to do so could make it difficult to enforce contractual terms because a court may find there was no binding contract.

With scraping, however, it may be more difficult for a party to dispute notice of a unilateral contract purporting to govern use of data or a database if the site or service has been accessed multiple times in connection with extracting data, or if the site or service has been targeted specifically.[13] Of course, where a site is accessed only once, or randomly by a bot or algorithm, rather than intentionally targeted for data extraction, the database owner may have a harder time establishing contract formation absent express assent.

Where database use or access is conditioned on acceptance of a unilateral contract, there is also a risk—particularly in more liberal jurisdictions such as California and in consumer (rather than commercial) contracts—that the contract or various provisions in the agreement could be challenged as unconscionable in the event of litigation. Readers should closely review sections 21.03, 21.04, 21.05, and 22.05[2][M] for guidance on when unilateral agreements may be held unenforceable as unconscionable.

Where an enforceable contract has been formed, a database owner may bring a breach of contract claim. In some circumstances where there is privity of contract and the defendant has thwarted the owner from benefiting from it, the database owner may bring a claim for breach of the duty of good faith and fair dealing, which under California law requires a showing that (1) the parties entered into a contract, (2) the plaintiff fulfilled its obligations under the contract, (3) any conditions precedent to the defendant's performance occurred, (4) the defendant unfairly interfered with the

---

[13] *See, e.g.*, *Domain Name Commission Ltd v. DomainTools, LLC*, 781 F. App'x 604, 606-07 (9th Cir. 2019) (affirming the lower court's preliminary injunction order, holding that DomainTools, a party accused of using data in violation of provisions in the terms of use of DNCL, the New Zealand nonprofit responsible for administering the.NZ Country Code Top Level Domain, was bound by DNCL's Terms of Use agreement, where "DNCL conspicuously displayed its terms of use in response to each of the hundreds of thousands of information requests DomainTools submitted[,]" where someone at DomainTools must have had actual knowledge of DNCL's terms of use, because DomainTools excised the terms of use appended to the information it received from DNCL before adding it to DomainTools' own database, and where DomainTools did not deny knowledge of the terms of use in response to DNCL's cease-and-desist letters).

plaintiff's rights to receive the benefits of the contract, and (5) the plaintiff was harmed by the defendant's conduct.[14] The implied covenant, however, is limited to assuring compliance with the express terms of a contract, and cannot be extended to create obligations not contemplated by it.[15] Nor can there be a breach of the duty of good faith and fair dealing if the conduct alleged was expressly permitted by the contract.[16]

Where a screen scraper or third party aggregator makes available software or other tools to allow users to circumvent restrictions in its contract, a database owner, in limited circumstances, also potentially may be able to bring claims for tortious interference with contract or interference with prospective economic advantage.[17] Where contract remedies may be unavailable, database owners have sought to assert claims for unjust enrichment,[18] although such claims, to the extent based on copying without an extra element, have been held preempted by the Copyright Act.[19]

---

[14]*See Herskowitz v. Apple, Inc.*, 940 F. Supp. 2d 1131, 1143 (N.D. Cal. 2013) (reciting the elements from a standard jury instruction).

[15]*See, e.g.*, *Herskowitz v. Apple, Inc.*, 940 F. Supp. 2d 1131, 1143 (N.D. Cal. 2013); *see generally infra* § 14.03[2] (discussing the doctrine and its application at greater length).

[16]*See, e.g.*, *Song Fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 885 (N.D. Cal. 2015) (granting Google's motion to dismiss claims for breach of YouTube's Terms of Service and breach of the duty of good faith and fair dealing arising out of plaintiffs' removal of a video where the Terms of Service permitted YouTube to remove the video "and eliminate its view count, likes, and comments"; "if defendants were given the right to do what they did by the express provisions of the contract there can be no breach [of the duty of good faith and fair dealing].").

[17]*See, e.g., Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1059–60 (N.D. Cal. 2010) (entering a default judgment for breach of contract, inducing breach of contract and intentional interference with contractual relations, where the defendants marketed a software product that allowed users to automate access to the Craigslist site, circumvent CAPTCHA restrictions and automatically and repeatedly post identical listings on Craigslist, and harvest email addresses, all in violation of Craigslist's TOU); *infra* § 5.03[5].

[18]*See, e.g., Information Handling Services, Inc. v. LRP Publications, Inc.*, No. CIV. A. 00-1859, Copy. L. Rep. (CCH) P28,177, 2000 WL 1468535 (E.D. Pa. Sept. 20, 2000) (denying a motion to dismiss a claim for unjust enrichment in a database copying case); *see generally infra* § 5.03[6].

[19]*See, e.g., Alan Ross Machinery Corp. v. Machinio Corp.*, No. 17-cv-3569, 2018 WL 3344364, at *6 (N.D. Ill. July 9, 2018) (dismissing Alan Ross Machinery's claim for unjust enrichment, in a case alleging that

In lieu of simple contracts, database agreements potentially may be cast as intellectual property licenses—even where the underlying data is unprotectable.[20] Many databases, even if comprised of unprotectable facts or data, may be entitled to copyright protection as compilations if there is sufficient creativity in the selection, arrangement or organization of the data.[21] Databases also frequently incorporate software that may be protected by copyright, trade secret and/or patent law and form the basis for an intellectual property license.

If a database agreement authorizes access to or use of intellectual property and therefore may be characterized as a license, rather than merely a contract, the agreement may be easier to enforce in some instances because courts generally allow rights owners to impose restrictions on licensees that might otherwise would be deemed impermissible in a regular contract (such as prohibitions on competition or reverse engineering[22]) as a condition of gaining access to intellectual property,[23] so long as the restrictions are not so severe that they amount to intellectual property misuse[24] or

---

Machinio scraped sales listings of industrial machinery from Alan Ross's website and duplicated those listings on its website, where it was "not clear how Machinio's listing of Alan Ross's machinery hurts Alan Ross. After all, Machinio is not a vendor, but rather a global search engine. Listing on Machinio's search engine would presumably benefit Alan Ross, by allowing more potential buyers and sellers to view the machinery."); *BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 618 (S.D.N.Y. 2010); *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 680–81 (N.D. Ohio 2010) (holding plaintiff's unjust enrichment claim preempted where it was based on the allegation that defendants took information). *But see Perfect 10, Inc. v. Google, Inc.*, No. CV04-9484, 2008 WL 4217837, at *9 (C.D. Cal. July 6, 2008) (holding plaintiff's unjust enrichment claim not preempted where the claim was premised on right of publicity and trademark violations); *see generally infra* § 5.03[6] (unjust enrichment); *supra* § 4.18[1] (analyzing copyright preemption).

[20]For a discussion of intellectual property licenses, *see infra* chapter 16.

[21]*See supra* § 5.02.

[22]*See infra* § 18.03[6].

[23]*See, e.g., Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) (enforcing website Terms of Use for access to a database as a copyright license); *see generally infra* § 21.03 & chapters 14, 16.

[24]*See infra* § 16.04.

violate antitrust laws.[25]

Where a database is entitled to copyright protection, a rights owner may have remedies against a licensee under both the Copyright Act (which potentially allows recovery of statutory damages and attorneys' fees[26]) and for breach of contract—or potentially only for breach of contract. Exceeding the scope of a valid license may be found to constitute infringement.[27] Likewise, violating a condition of the license may be deemed copyright infringement, rather than merely a breach of contract.[28] Other breaches of a license agreement, however, may be deemed merely contractual, and would not afford independent grounds for a database owner to sue for copyright infringement in federal court or seek statutory damages or attorneys' fees. Whether and to what extent a contractual restriction may be considered a condition of the license, rather than merely contractual, is analyzed in section 14.06[2].

Even where an agreement is merely a contract for access to data, some courts will enforce use restrictions on the theory that the database owner was not required to grant access to the database in the first place, and that the licensee knowingly gave up certain rights that it otherwise may have had with respect to its use of unprotectable data, in return

---

[25]*See infra* chapter 34.

[26]*See supra* §§ 4.14, 4.15. As discussed in section 4.14, statutory damages, if available, allow a plaintiff to recover up to $150,000 per work infringed where willful infringement may be shown and typically are sought where actual damages would be negligible or would be difficult or expensive to prove.

[27]*See, e.g., I.A.E., Inc. v. Shaver*, 74 F.3d 768, 775 (7th Cir. 1996); *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 517 (9th Cir. 1993), *cert. dismissed,* 510 U.S. 1033 (1994); *see generally supra* § 4.08[5]; *infra* § 14.06[2].

[28]*See MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 629 F.3d 928, 939-41 (9th Cir. 2010) (holding that Terms of Use restrictions on the use of bots—or intelligent agent software—as a form of "cheating" to acquire virtual goods in World of Warcraft, was a contractual covenant, rather than a condition of the license, and therefore could not form the basis for a claim for copyright infringement when breached). For a licensee's violation of a contract to constitute copyright infringement, according to the Ninth Circuit, there must be a nexus between the condition and the licensor's exclusive rights of copyright. Otherwise, "any software copyright holder . . . could designate any disfavored conduct during software use as copyright infringement by purporting to condition the license on the player's abstention from the disfavored conduct." *Id.* at 941; *see generally infra* § 16.02[1] (analyzing this issue in greater detail).

for obtaining the right to access and use the database.[29] Some judges, however, will strain to find copying permissible if undertaken for the purpose of accessing unprotectable data,[30] so in practice, even if not necessarily as a matter of black letter law, database owners are better off including restrictions in IP licenses, rather than mere access contracts, and obtaining express assent, where possible.

The major cases involving database contracts and licenses are analyzed below in section 5.03[2]. Readers are cautioned, however, to closely review chapters 21 (especially sections 21.03, 21.04 and 21.05) and 22 on unilateral contracts, which provide a broader perspective on the enforceability of database EULAs and Terms of Use.

Whether an agreement fully protects a database owner, or leaves opportunities for a third party to copy or use the contents of the database, also depends on the particular use restrictions imposed by the agreement. Use restrictions are addressed in section 5.03[2], as well as in *Ticketmaster LLC v. RMG Technologies, Inc.*,[31] which is discussed in section 5.03[2].

5.03[2] Database Contract Case Law

The first case to construe a database contract involving Internet use was *ProCD, Inc. v. Zeidenberg*,[1] which was decided in 1996. In that case, the Seventh Circuit upheld the enforceability of a non-negotiated, pre-printed shrinkwrap license, which had been included with a CD-ROM containing a database of unprotectable information compiled from telephone directories.[2]

Judge Easterbrook assumed, for purposes of the case, that

---

[29] *See, e.g., Information Handling Services, Inc. v. LRP Publications, Inc.*, No. CIV. A. 00-1859, Copy. L. Rep. (CCH) P28,177, 2000 WL 1468535 (E.D. Pa. Sept. 20, 2000).

[30] *See supra* § 5.02.

[31] *Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

[Section 5.03[2]]

[1] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

[2] The CD-ROM also included a protectable software program that allowed users to search the database, but the Seventh Circuit's opinion focused on the defendant's reproduction of the database on a website. The facts of the case are set forth in greater detail in connection with the enforceability of unilateral licenses. *See infra* § 21.02, § 21.03.

ProCD's database, although more complex and voluminous than a regular telephone directory (which included, for example, full nine-digit zip codes and census industrial codes), nonetheless was unprotectable under *Feist Publications, Inc. v. Rural Telephone Service Co.*[3] Notwithstanding this ruling, the Seventh Circuit held that ProCD's purely factual database could be effectively protected by a shrink-wrap license.

The legal authority for this aspect of the court's ruling, however, was not clearly articulated. Judge Easterbrook cited trade secret cases such as *Kewanee Oil Co. v. Bicron*,[4] and *Aronson v. Quick Point Pencil Co.*[5] for the proposition that ProCD's shrinkwrap license was enforceable to limit defendants' use of ProCD's otherwise unprotectable database. Moreover, in connection with his discussion of the Aronson case, Judge Easterbrook referred to directories collected for inclusion in a hypothetical database as "intellectual property." Yet in the *Zeidenberg* case itself there is no suggestion that plaintiff's database constituted a trade secret, or that it was otherwise protectable. In fact, to the contrary, the district court, in analyzing plaintiff's cause of action for misappropriation, emphasized that plaintiff's claim was based on common law misappropria-

---

[3] *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991).

[4] *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974).

[5] *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257 (1979). *Aronson* involved a license to a novel invention, which provided for different license fees depending on whether the licensor was able to obtain a patent. When a patent could not be obtained, the licensee sought a declaration that the license agreement was unenforceable. In upholding the agreement under the lower license fee (since the licensor was unsuccessful in obtaining a patent), the Supreme Court emphasized that the invention was secret before the licensee commercially exploited it, which allowed the licensee to profit from being first in the market. *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257, 265–66 (1979), *citing Kewanee Oil Co. v. Bicron* 416 U.S. 470 (1974); Restatement of Torts § 757, Comment b. Thus, *Aronson* is a case firmly grounded in trade secret law.

A broad reading of *Aronson* (and perhaps the one implicitly intended by Judge Easterbrook) would also support the proposition that a licensee who accepts something of value that a licensor is not required to provide is thereafter bound by the terms of its license agreement, which is consistent with the rationale provided by some courts (in cases cited in this section and in section 18.06) in enforcing contracts that restrict use of otherwise unprotectable data.

tion of trade secrets.[6]

Courts analyzing database licenses since *Zeidenberg* typically have either enforced end user license agreements as valid contracts or licenses or raised concerns about the implications of restricting access to publicly available information. Databases often include software or other intellectual property that must be used to access the data in a database, thus justifying imposing restrictions on the use of otherwise unprotectable data. Most courts seem comfortable with the notion that a licensee may be bound by restrictions on otherwise unprotectable data if its access to the data was provided pursuant to an agreement that granted it rights that the licensor otherwise could freely withhold (especially if the agreement granted access to intellectual property—such as software—or a database protectable based on the selection, arrangement or organization of its contents). On the other hand, attempts to expand the monopoly power granted a copyright owner to unprotectable material could prevent a licensor from enforcing its rights under the copyright misuse doctrine.[7]

Judge Easterbrook's own opinion in *ProCD, Inc. v. Zeidenberg* underscores the tension between enforcing contract rights and protecting access to unprotected data. For example, under Judge Easterbrook's analysis, Borland, which copied the unprotectable menu command hierarchy of Lotus' Lotus 1-2-3 program and was exonerated by an equally divided Supreme Court in *Lotus Dev. Corp. v. Borland Int'l, Inc.*,[8] could have been subjected to liability if, instead of proceeding under copyright law, Lotus had sued Borland for violation of a shrinkwrap license that prohibited copying except for personal use. Moreover, in the *Zeidenberg*

---

[6] *ProCD, Inc. v. Zeidenberg*, 908 F. Supp. 640, 660 (W.D. Wis. 1996), *rev'd*, 86 F.3d 1447 (7th Cir. 1996). Plaintiff's database was comprised of public phone book entries and therefore was not secret. The software developed to manage the data arguably could have constituted or embodied a trade secret. *See infra* § 10.03.

[7] *See, e.g., Lasercomb America, Inc. v. Reynolds*, 911 F.2d 970, 978 (4th Cir. 1990); *DSC Communications Corp. v. DGI Technologies, Inc.*, 81 F.3d 597, 601 (5th Cir. 1996); *Practice Management Information Corp. v. American Medical Ass'n*, 133 F.3d 1140 (9th Cir. 1998), *cert. denied*, 522 U.S. 933 (1998). For an analysis of intellectual property misuse doctrines, *see infra* § 16.04.

[8] *Lotus Development Corp. v. Borland Int'l, Inc.*, 49 F.3d 807 (1st Cir. 1995), *aff'd mem.*, 516 U.S. 233 (1996) (4-4 decision); *see generally supra* § 4.07.

case itself, although ProCD sought to enjoin defendants' copying of the telephone listings contained on its CD-ROM, ProCD—ironically—would not have been able to compile its CD-ROM listings from over 3,000 telephone books, royalty free, had it not, like *Zeidenberg*, relied on the Supreme Court's ruling in *Feist* that phone book compilations are unprotectable under U.S. copyright law. In holding that access to unprotectable data may be restricted by a shrinkwrap license, the Seventh Circuit seems to have condoned ProCD's copying of unprotectable data from a phone book, while penalizing Zeidenberg for essentially the same conduct. It is doubtful that this was the intended consequence of the Seventh Circuit's otherwise well-reasoned opinion.

In *Hill v. Gateway 2000, Inc.*,[9] Judge Easterbrook suggested that the *Zeidenberg* decision rested on the UCC and expressly rejected the notion that the sweeping restrictions enforced in *Zeidenberg* were in any way justified by license (and hence underlying intellectual property), rather than merely by contract.

In *Register.com, Inc. v. Verio, Inc.*,[10] the Second Circuit held that Verio was bound by Register.com's posted Terms, even though express assent was neither sought nor obtained, because Verio acknowledged that it was aware that *Register.com* purported to condition use of its site on posted Terms. In that case, *Register.com*, a domain name registrar, was contractually required to make the contact information of domain name registrants from the WHOIS database available free of charge to the public for any lawful purpose. When the database was queried, however, *Register.com* displayed a purported restriction on use in the results screen. Specifically, users were shown a restrictive legend purporting to prohibit recipients from using the data to transmit "mass unsolicited, commercial advertising or solicitation via email" (or in connection with mail or telephone solicitations).[11]

Verio used bots (or intelligent agent software) to access

---

[9] *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997).

[10] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004).

[11] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 396 (2d Cir. 2004). Register.com initially prohibited solicitation by email, mail or telephone. Its agreement with ICANN, however, prohibited it from restricting access to the data for any lawful purpose except mass unsolicited email. *See infra* § 7.02. Register.com therefore narrowed its policy to just prohibiting email solicitations.

the site and copy the contact information of new registrants, who it then solicited via email, telemarketing and direct mail marketing solicitations.

Verio acknowledged that it was aware of the restrictions that *Register.com* purported to impose on users, but argued that it was not bound by them because the legend did not appear on the screen until after Verio had queried the database and received the desired information. Judge Leval, writing for a majority of the panel, however, found Verio bound by the terms, writing that:

> It is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree.[12]

In *Information Handling Services v. LRP Publications, Inc.*,[13] the court stated in *dicta* in ruling on a motion to dismiss that a shrinkwrap license restricting use of a CD-ROM and its contents was enforceable in preventing the defendant from copying material that was not protected by copyright law. The specific issue in that case was whether plaintiffs' claims against a competing database company were preempted by the Copyright Act. The plaintiffs alleged that the defendant, through an employee, subscribed to plaintiffs' PERSONNET database (a database that included material such as decisions by the Equal Employment Opportunity Commission (EEOC)) by falsely representing herself as an attorney who intended to use the product in her practice. In fact, the employee allegedly intended all along to use her access to the database to engage in wholesale copying, which is what in fact she did. The court

---

With respect to the earlier policy, the Second Circuit rejected Verio's argument that it could not be held liable for telephone and mail solicitations given the terms of Register.com's agreement with ICANN because that agreement provided that there were no third-party beneficiaries. The Second Circuit therefore analyzed Verio's potential liability on the assumption that Register.com was legally authorized to demand that users of WHOIS data from its system refrain from using it for mass solicitation by mail and telephone, as well as by email.

[12] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 403 (2d Cir. 2004) (citing multiple sources). The *Verio* case is discussed in greater detail in section 21.03.

[13] *Information Handling Services, Inc. v. LRP Publications, Inc.*, No. CIV. A. 00-1859, Copy. L. Rep. (CCH) P28,177, 2000 WL 1468535 (E.D. Pa. Sept. 20, 2000).

dismissed a claim for "misappropriation and unfair competition," finding that it alleged copying without an extra element and was therefore preempted.[14] The court, however, denied defendant's motion with respect to claims for breach of contract, tortious interference with contractual relations, conspiracy, tortious interference with prospective contractual relations, unjust enrichment, fraud and unfair competition/misappropriation of trade secrets.

In addressing plaintiff's breach of contract claim, Judge Fullam wrote that while copyright law does not allow a database owner to prevent third parties from copying unprotectable material simply because it took time and effort to create it, "there is no law that requires [a database owner] to make [its] product publicly available; nor is it permissible to break into [a] house and steal it in order to copy the material it contains." He further observed:

> I am not unmindful of the concern that enforcing licenses such as the one involved here, which are not-bargained-for and are offered with the product on a take-it-or-leave-it basis, may be the functional equivalent of expanding, under the rubric of various state laws, copyright protection to otherwise uncopyrightable materials. *See* 1 Melville B. Nimmer & David Nimmer, Nimmer on Copyright, § 3.04[B][3][a]. In the absence of congressional guidance, however, I can see no reason not to enforce the contract under the circumstances presented in this case. It is not unconscionable. Defendant . . . was free to reject it and return the CD-ROM disc to [plaintiffs]. Defendant chose not to do so, and therefore is bound by its terms."

In unreported but widely discussed opinions in *Ticketmaster Corp. v. Tickets.com, Inc.*,[15] a district court case that was the first one to consider the effectiveness of posted Terms of Use, the court initially dismissed Ticketmaster's breach of contract claim against *Tickets.com* where Ticketmaster's TOU were accessible via a link that appeared in "small print" on the bottom of Ticketmaster's home page, but granted leave for Ticketmaster to amend its complaint to allege that *Tickets.com* had knowledge of the terms and impliedly agreed to them.[16] Thereafter, Ticketmaster changed the placement of the link to its notice to a prominent place on its homepage

---

[14] *See infra* § 5.04.

[15] *Ticketmaster Corp. v. Tickets.com, Inc.*, CV 99-7654 HLH (BQRx), 2000 WL 525390 (C.D. Cal. Mar. 27, 2000), *aff'd mem.*, Appeal No. 00-56574 (9th Cir. Jan. 2001).

[16] Ticketmaster had sought to prevent *Tickets.com*, a competitor, from

and warned users that proceeding beyond the homepage would be deemed agreement to Terms of Use that prohibited commercial use of the site.[17] Ticketmaster also reiterated the conditions imposed on access to its site in a letter to *Tickets.com*.

In a subsequent decision,[18] the court denied the defendant's motion for summary judgment on Ticketmaster's breach of contract claim, finding that a contract could have been formed when *Tickets.com* proceeded into the interior of the Ticketmaster site after knowing of the conditions imposed by Ticketmaster for doing so. In so ruling, the court emphasized that *Tickets.com* was "fully familiar with the conditions [Ticketmaster] claimed to impose on users," citing in particular Ticketmaster's letter and a response from *Tickets.com* stating that it did not accept the conditions, as well as the new and more prominent notice placed on Ticketmaster's homepage. The court ruled that there was sufficient evidence to defeat summary judgment "if knowledge of the asserted conditions of use was had by [Tickets.com], who nevertheless continued to send its spider into the [Ticketmaster] interior Web pages, and if it is legally concluded that doing so can lead to a binding contract."

The Ticketmaster court lamented the result of its ruling, expressing a preference for "a rule that required an unmistakable assent to the conditions easily provided by requiring clicking on an icon which says 'I agree' or the equivalent." It acknowledged, however, that "the law has not developed in this way" and that "no particular form of words is necessary to indicate assent—the offeror may specify that a certain action in connection with his offer is deemed acceptance, and [the offer will] ripe[n] into a contract when the action is

---

deep linking to internal pages on its website and from using bots to spider or crawl pages on its site and electronically extract factual information from the Ticketmaster site. *See infra* § 9.06 (discussing the case at greater length in connection with linking).

[17]The notice read:

> Use of this site is subject to express terms of use, which prohibit commercial use of this site. By continuing past this page, you agree to abide by these terms.

[18]*Ticketmaster Corp. v. Tickets.com, Inc.*, CV99-7654-HLH (VBKx), 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).

taken."[19]

In a later case also brought by Ticketmaster, *Ticketmaster LLC v. RMG Technologies, Inc.*,[20] Ticketmaster was able to enforce its Terms against a user who acknowledged it was aware of the restrictions and the court treated the posted Terms as an intellectual property license. The case is instructive both for contract formation and the terms of the database license that the court enforced.

In *RMG Technologies, Inc.*, Judge Audrey Collins, ruling on a motion for preliminary injunction, ruled that Ticketmaster was likely to prevail on the merits in establishing that a competitor had notice of posted Terms of Use but nonetheless accessed and used the Ticketmaster website in violation of those Terms. The court characterized Ticketmaster's Terms as creating a non-exclusive copyright license to Ticketmaster's copyrighted website. In addition, the homepage to the site included the warning that "[u]se of this website is subject to express Terms of Use which prohibit commercial use of this site. By continuing past this page, you agree to abide by these terms." The underlined phrase "Terms of Use" was a hyperlink to the full Terms of Use. In addition, the same phrase appeared on almost every page of the Ticketmaster site. Further, since 2003 users had to affirmatively agree to the Terms as part of the procedure for setting up an account and since mid-2006 had to expressly assent to the Terms any time they purchased tickets from the site. The defendant acknowledged that it had notice of the Terms of Use but argued that it was not bound by them and they were too vague to be enforced, which the court rejected. Because the defendant acknowledged that it was on notice of the Terms, the court found that it had assented to be bound by the Terms by using the website.

Ticketmaster's Terms of Use included a number of provisions expressly intended to thwart competitors from access-

---

[19]*Ticketmaster Corp. v. Tickets.com, Inc.*, CV99-7654-HLH (VBKx), 2003 WL 21406289, at *2 (C.D. Cal. Mar. 7, 2003) (citing other cases). In addition to Internet contract cases, the court cited the shrinkwrap cases (*see infra* § 21.02), *Carnival Cruise Lines, Inc. v. Shute*, 499 U.S. 585 (1991) (*see infra* §§ 21.02, 21.03, § 53.03[2]), and the fact that "[t]he Carriage of Goods by Sea Act, the Carmack Act, and the Warsaw Convention provide that limitations of liability on the bill of lading, air waybill, or airplane ticket are enforceable if the services are used by the customer."

[20]*Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

ing and copying its database. The Terms, among other things prohibited commercial use of the Ticketmaster website, including duplication or downloading of material, and purported to license only personal, non-commercial use.[21] The Terms also prohibited the use of bots or other automated devices.[22] The agreement also included an undertaking by the user "not [to] take any action that imposes an unreasonable or disproportionately large load on our infrastructure."[23] To further limit automated copying, the Terms included an undertaking not to access the site more than once during any three second interval.[24] For good measure, the Terms made clear that users "do not have permission to access this site in any way that violates . . . these terms of use."[25] The Terms also provided that users understood and agreed that Ticketmaster could terminate their access to the site or cancel their ticket orders or the actual tickets acquired through the site if Ticketmaster believed that the conduct of a user or anyone who Ticketmaster believed was acting in concert with the user violated or was inconsistent with the Terms of Use or the law or violated the rights of Ticketmaster, a client of Ticketmaster or another user of the site.

In *RMG Technologies, Inc.*, the defendant used bots or another automated means to access the Ticketmaster site and extract information from its database. Although the defen-

---

[21]The relevant provisions included the following:

> You [the viewer] agree that you are only authorized to visit, view and to retain a copy of pages of this site for your own personal use, and that you shall not duplicate, download, [or] modify . . . the material on this site for any purpose other than to review event and promotions information, for personal use . . . . No . . . areas of this site may be used by our visitors for any commercial purposes.

[22]The Terms stated:

> You agree that you will not use any robot, spider or other automated device, process, or means to access the site . . . . You agree that you will not use any device, software or routine that interferes with the proper working of the site nor shall you attempt to interfere with the proper working of the site.

[23]*Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096, 1107 (C.D. Cal. 2007).

[24]The Terms provided:

> You agree that you will not access, reload or "refresh" transactional event or ticketing pages, or make any other request to transactional servers, more than once during any three-second interval.

[25]*Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096, 1108 (C.D. Cal. 2007).

dant denied using automated means, Ticketmaster's expert showed that several webpage requests per second were made to Ticketmaster from the same IP address, amounting to thousands of requests per day that were too numerous to have been generated in a manual, non-automated way. In addition, the defendant advertised a product called PurchaseMaster as "do[ing] the work of a dozen people at once." Accordingly, the court found Ticketmaster likely to prevail based on the defendant's use of an automated device in violation of the Terms of Use, as well as the provisions restricting access to once every three seconds. Because the court deemed the Terms of Service a license to Ticketmaster's copyrighted site, the defendant's access beyond what was permitted by the license also was potentially a copyright violation.

RMG Technologies, Inc., was followed by the court in *Facebook, Inc. v. Power Ventures, Inc.*,[26] in which Judge Jeremy Fogel of the Northern District of California denied defendants' motion to dismiss copyright and DMCA claims arising out of their screen scraping user data from Facebook's website. In that case, defendants operated a website that allowed users to access their accounts on various different email services and social networks from a single location using screen-scraping tools.

The court ruled that Facebook stated claims based on defendants exceeding the scope of permissible access, as defined by Facebook's Terms of Use agreement.[27] Among other things, Facebook's Terms of Use agreement granted a limited license to users to access the site and service, but only on the terms specifically authorized in the TOU agreement.[28] The agreement also prohibited harvesting or collecting email addresses or other contact information by electronic or other means for the purpose of sending unsolicited emails or other unsolicited communications. Facebook's Terms of Use agreement further broadly prohibited the downloading, scraping, or distributing of any content on the website (except that users were permitted to download

---

[26]*Facebook, Inc. v. Power Ventures, Inc.*, 91 U.S.P.Q.2d 1430, 2009 WL 1299698 (N.D. Cal. May 11, 2009).

[27]*See infra* § 5.08 (discussing Facebook's Lanham Act claim).

[28]The relevant provision stated that "[a]ny use of the site or the site content other than as specifically authorized herein, without the prior permission of the company, is strictly prohibited and will terminate the license granted herein."

their own content). It also prohibited "data mining, robots, scraping, or similar data gathering or extraction methods" (with no exception to this prohibition for user access).

Database access restrictions in Craigslist's TOU also were enforced against defendants who accessed the site in excess of TOU restrictions to harvest email addresses and develop and market software and related services to allow users to automate the process of posting listings on Craigslist.[29] In that case, the court granted a default judgment on claims for breach of the TOU as well as for inducing breach of contract and intentional interference with contractual relations (based on breaches of the TOU by users of defendants' automated software programs).

In *Health Grades, Inc. v. Robert Wood Johnson University Hospital, Inc.*,[30] the court held that plaintiff's claim that the defendant hospital breached its click-through license agreement with the plaintiff by commercially reproducing, modifying and/or distributing its own healthcare provider award and ranking information from plaintiff's website in press releases and other marketing materials was preempted, but that its breach of contract claim based on unauthorized use of the plaintiff's mark in a way that implied that the owner endorsed the hospital's services was not preempted and could proceed. In that case, the defendant had accessed and clicked assent to plaintiff's limited license more than 200 times.

Similarly, in *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*,[31] the court denied in part defendant's summary judgment motion, holding that a reasonable jury could conclude that the defendant had actual or constructive knowledge of the Snap-on EULA where defendant accessed Snap-on's websites, which contained a single page access screen where users were required to input their user names and passwords and then click an "Enter" button to proceed,

---

[29] *See Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039 (N.D. Cal. 2010) (entering a default judgment for copyright infringement, trademark infringement based on use on plaintiff's marks in sponsored links, circumvention (of CAPTCHA) under the DMCA, exceeding authorized access under the CFAA (based on exceeding permitted access under Craigslist's TOU), breach of contract (based on the TOU), fraud and violations of Cal. Penal Code § 502).

[30] *Health Grades, Inc. v. Robert Wood Johnson University Hosp., Inc.*, 634 F. Supp. 2d 1226, 1242–47 (D. Colo. 2009).

[31] *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 681–83 (N.D. Ohio 2010).

below which was found the message that "[t]he use of and access to the information on this site is subject to the terms and conditions set forth in our legal statement" and a green box with an arrow that users could click to access the EULA. The EULA restricted access to the site to authorized dealers, customers or other licensees, and there was no dispute that O'Neil, a competitor which entered the site, was none of these, although the parties disputed whether O'Neil was an authorized agent for Mitsubishi, a customer of both O'Neil and Snap-on, and whether Mitsubishi was authorized to access the site.[32]

Online and mobile contract formation is addressed more extensively in section 21.03.

5.03[3] The Scope of Contractual Restrictions

Database agreements typically restrict access to and use of a database but may not necessarily prohibit all uses of data. Some broadly restrict commercial use of a database, such as the agreements at issue in *Ticketmaster LLC v. RMG Technologies, Inc.*[1] and *Facebook, Inc. v. Power Ventures, Inc.*,[2] which were discussed above in section 5.03[2]. The access and use restrictions in those agreements, which are discussed in section 5.03[2], should be closely reviewed.

Other database agreements, however, do not broadly restrict commercial use (often times because the agreement by its nature is intended to provide access for business uses). Some agreements include confidentiality provisions with carve outs for information that is in the public domain, which

---

[32]Snap-On eventually obtained a general jury verdict at trial, although it is not clear whether the verdict was based on Snap-On's claim for breach of the EULA or other claims for trespass, copyright infringement or violations of the Computer Fraud and Abuse Act. *See Snap-On Business Solutions Inc. v. O'Neil & Associates, Inc.*, No. 5:09–CV–1547, 2010 WL 2650875 (N.D. Ohio July 2, 2010) (awarding costs but denying Snap-On's request for an award of attorneys' fees because under Ohio law contractual attorneys' fee provisions are unenforceable as contrary to public policy because they are viewed as encouraging litigation); *see generally infra* § 5.05[1] (discussing the facts of the case and other rulings in greater detail).

[Section 5.03[3]]

[1]*Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

[2]*Facebook, Inc. v. Power Ventures, Inc.*, 91 U.S.P.Q.2d 1430, 2009 WL 1299698 (N.D. Cal. May 11, 2009).

may include factual material in a database. This type of provision is especially common where mutual confidentiality obligations are imposed or in unilateral agreements where drafters may be concerned about avoiding one-sided provisions that appear unconscionable. Other confidentiality provisions may be more akin to trade secret licenses, which tightly restrict information which, while potentially unprotectable under copyright law, may have great value so long as kept secret.[3]

To determine whether and to what extent the contents of a database may be used, lawyers should, among other terms, review:

- The scope of the grant clause (to determine exactly what aspects of the database are deemed subject to the license and what restrictions, if any, are imposed in the grant clause itself);
- The Term and Termination provisions (which may specify rights following termination or require return or destruction of all data);
- Confidentiality provisions, which may exclude certain categories of information, broadly include even factual data or explicitly include only certain information (thereby impliedly allowing the use of other material in the database, unless restricted by another provision in the agreement); and
- Use restrictions, which may purport to restrict or permit certain uses.

What a contract provides ultimately may present a question of fact precluding summary judgment—and requiring a trial to determine—if the terms are not adequately defined in the agreement itself.[4]

5.03[4] Forms

A sample database EULA is included in the appendix to

---

[3] *See generally infra* § 10.04[3] (analyzing NDAs in connection with trade secret protection).

[4] *See, e.g., Meridian Project Systems, Inc. v. Hardin Const. Co., LLC*, 426 F. Supp. 2d 1101, 1109–10 (E.D. Cal. 2006) (denying summary judgment on the issue of whether the defendant breached a license that prohibited copying "software or documentation" where it was undisputed that the defendant copied the "help" file, but where the court found that text and instructions in the Help file could constitute either, neither or both software and documentation).

chapter 21. Sample Terms of Service agreements governing access and use of websites are included in the appendix to chapter 22.

5.03[5] Interference with Contract or Prospective Economic Advantage

A claim for tortious interference with contract may be asserted if a defendant induces a third party to breach a database access agreement.[1] A claim for tortious interference with contract or interference with prospective economic advantage also may be asserted if a third party makes available software or other tools to allow users to circumvent restrictions in a database agreement or website Terms of Use.[2] Merely scraping sales listings and copying them to another website will be insufficient to state a claim.[3]

[Section 5.03[5]]

[1]*See Thomson Reuters Enterprise Centre GmbH v. ROSS Intelligence Inc.*, ___ F. Supp. 3d ___, 2021 WL 1174725, at *8 (D. Del. 2021) (denying ROSS's motion to dismiss where Thomson Reuters alleged that LegalEase had a contract with West, which ROSS knew, and that ROSS nonetheless pursued LegalEase "to acquire access to and copy Plaintiffs' valuable content" while "knowing that it violated the terms of LegalEase's contract with West.").

[2]*See, e.g., Craigslist Inc. v. Kerbel*, No. C-11-3309, 2012 WL 3166798 (N.D. Cal. Aug. 2, 2012) (entering a default judgment for breach of contract and inducing breach of contract, in addition to violations of the DMCA and the Lanham Act, where the defendant sold a service designed to automatically post to craigslist and circumvent its CAPTCHA restrictions, in violation of Craigslist's TOU); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1059–60 (N.D. Cal. 2010) (entering a default judgment for breach of contract, inducing breach of contract and intentional interference with contractual relations, where the defendants marketed a software product that allowed users to automate access to the Craigslist site, circumvent CAPTCHA restrictions and automatically and repeatedly post identical listings on Craigslist, and harvest email addresses, all in violation of Craigslist's TOU).

[3]*See, e.g.*, *Alan Ross Machinery Corp. v. Machinio Corp.*, No. 17-cv-3569, 2018 WL 3344364, at *6 (N.D. Ill. July 9, 2018) (dismissing Alan Ross Machinery's claim for tortious interference with prospective business advantage under Illinois law, in a case alleging that Machinio scraped sales listings of industrial machinery from Alan Ross's website and duplicated those listings on its website, where Alan Ross did not allege that Machinio directed its conduct at Alan Ross's business prospects to induce them to end their relationship with Alan Ross and where Machinio did not sell the machinery—it connected buyers and sellers, "presumably helping Alan Ross, a vendor, to buy and sell more machinery through additional marketing. Alan Ross has failed to plausibly allege that Machinio

A database owner may sue a third party for breach of its database or website access or use agreement, but generally only if there is privity of contract. However, if a screen scraper or aggregator is not itself engaged in these practices, and merely makes available the tools for others to use, the database owner potentially may seek to sue the third party directly based on interference claims, provided the restrictions being circumvented are part of an enforceable contract[4] and the third party has knowledge of its existence.

While the elements of these claims may vary somewhat from state to state, they typically require a showing of a contract, knowledge, interference and damage (or in the case of prospective economic advantage, merely harm to potential business relationships, rather than interference with an existing contractual relationship). For example, to prevail in California on a claim for intentional inducement to breach a contract, a plaintiff must prove: (1) the existence of a valid contract between the plaintiff and a third party; (2) the defendant's knowledge of this contract; (3) intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the relationship; and (5) resulting damage.[5] Under California law, a defendant's conduct need not be wrongful apart from the interference with contract[6] (although, by contrast, a plaintiff must show wrongfulness to state a claim for interference

---

intended to induce a third party to end its relationship with Alan Ross.").

[4]*See supra* §§ 5.03[1], 5.03[2]; *see generally infra* §§ 21.03, 21.04 (analyzing the enforceability of unilateral contracts, click-to-accept agreements and posted Terms).

[5]*See Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1059 (N.D. Cal. 2010), *citing Quelimane Co. v. Stewart Title Guaranty Co.*, 19 Cal. 4th 26, 55, 77 Cal. Rptr. 2d 709, 960 P.2d 513 (1998) and *Metal Lite, Inc. v. Brady Const. Innovations, Inc.*, 558 F. Supp. 2d 1084, 1094 (C.D. Cal. 2007); *Little v. Amber Hotel Co.*, 202 Cal. App. 4th 280, 291 (Cal. App. 2011).

[6]*Quelimane Co. v. Stewart Title Guaranty Co.*, 19 Cal. 4th 26, 77 Cal. Rptr. 2d 709, 726, 960 P.2d 513 (1998). To show the requisite level of intent, it is not necessary that plaintiffs prove that the primary purpose of defendant's conduct was the interference with contract. *Quelimane*, 77 Cal. Rptr. 2d at 727. Rather, it is sufficient to show that the defendant knew that the interference was certain or substantially certain to occur as the result of his action. *Quelimane*, 77 Cal. Rptr. 2d at 727; *see also Davis v. Nadrich*, 174 Cal. App. 4th 1, 10, 94 Cal. Rptr. 3d 414 (2d Dist. 2009) ("The rule applies . . . to an interference that is incidental to the actor's independent purpose and desire but known to him to be a necessary consequence of his action."; *quoting Korea Supply Co. v. Lockheed Martin*

with prospective economic advantage).[7] California also recognizes an analogous cause of action for tortious interference with contract, which is similar to intentional inducement, but does not require a showing that the contract actually was breached (disruption of the contractual relationship is sufficient).[8]

To state a claim for interference with prospective economic advantage under California law, a plaintiff must show interference with *existing* noncontractual relations which hold the promise of future economic advantage.[9] To prove interference with prospective economic advantage, a plaintiff must establish: (1) an economic relationship between the plaintiff and some third party, with the probability of future economic benefit to the plaintiff; (2) the defendant's knowledge of the relationship; (3) intentional acts on the part of the defendant designed to disrupt the relationship; (4) actual disruption of the relationship; and (5) economic harm to the plaintiff proximately caused by the acts of the defendant.[10] Unlike other contract-based torts, under California law a plaintiff also must show that "the defendant engaged in conduct that was wrongful by some legal measure, independent of its impact on the prospective relationship." "A plaintiff must also show that the defendant's conduct was independently unlawful, that is, 'proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard.' "[11]

Under Ohio law, tortious interference with a business re-

Corp., 29 Cal. 4th 1134, 1155–56, 131 Cal. Rptr. 2d 29 (2003)).

[7]*See, e.g., Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 131 Cal. Rptr. 2d 29 (2003).

[8]*See Winchester Mystery House, LLC v. Global Asylum, Inc.*, 210 Cal. App. 4th 579 (2012).

[9]*See, e.g., KEMA, Inc. v. Koperwhats*, 658 F. Supp. 2d 1022, 1034 (N.D. Cal. 2009), *citing Westside Center Associates v. Safeway Stores 23, Inc.*, 42 Cal. App. 4th 507, 524, 528, 49 Cal. Rptr. 2d 793 (5th Dist. 1996) (holding that the plaintiff failed to state a claim based on interference with "with the entire market of all possible but yet unidentified buyers for its property" because the tort "protects the expectation that the relationship will eventually yield the desired benefit, not necessarily the more speculative expectation that a potentially beneficial relationship will eventually arise.").

[10]*Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1153 (2003).

[11]*Little v. Amber Hotel Co.*, 202 Cal. App. 4th 280, 292 n.7 (Cal. App. 2011); *see also Winchester Mystery House, LLC v. Global Asylum, Inc.*, 210

lationship may be established by evidence of (1) a business relationship, (2) the tortfeasor's knowledge of the relationship, (3) an intentional interference causing a breach or termination of the relationship, and (4) resulting damages.[12] Similarly, under Washington law, a party claiming tortious interference with a contractual relationship or business expectancy must prove: (1) the existence of a valid contractual relationship or business expectancy; (2) that defendants had knowledge of that relationship; (3) an intentional interference inducing or causing a breach or termination of the relationship or expectancy; (4) that defendants interfered for an improper purpose or used improper means; and (5) resultant damage.[13]

Under Tennessee law, the test is stated somewhat more strictly as requiring: (1) an existing business relationship with specific third parties or a prospective relationship with an identifiable class of third persons; (2) the defendant's knowledge of that relationship and not a mere awareness of the plaintiff's business dealings with others in general; (3) the defendant's intent to cause the breach or termination of the business relationship; (4) the defendant's improper motive or improper means; and finally, (5) damages resulting from the tortious interference.[14]

In some states, including Florida, only strangers to a contract or business relationship may be held liable for tortious interference.[15]

While knowledge may be inferred based on the nature of the product (such as one targeted directly at a particular database or website), it may also be established expressly by sending the third party a letter or email unambiguously placing it on notice of the restrictions and allowing it a reasonable time to discontinue objectionable practices.

Interference with contract claims may be more difficult to

Cal. App. 4th 579 (2012); *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1159 (2003).

[12]*Jedson Engineering, Inc. v. Spirit Const. Services, Inc.*, 720 F. Supp. 2d 904 (S.D. Ohio 2010).

[13]*Pacific Northwest Shooting Park Ass'n v. City of Sequim*, 158 Wash. 2d 342, 351 (2006).

[14]*Trau–Med of Am., Inc. v. Allstate Ins. Co.*, 71 S.W.3d 691, 701 (Tenn. 2002).

[15]*See, e.g.*, *Alticor v. UMG Recordings, Inc.*, No. 6:14-cv-542-Orl-37DAB, 2015 WL 736346, at * 3 (M.D. Fla. Feb. 20, 2015).

establish, however, where a contract is terminable at will.[16]

Interference claims also may be hard to establish where the injury is *de minimis*. In *Fields v. Wise Media, LLC*,[17] for example, Northern District of California Judge William Alsup dismissed plaintiffs' intentional interference with contract claim without leave to amend where they alleged that defendants interfered with their mobile phone contracts by sending them unsolicited text messages that they knew would likely cause them to incur charges. Judge Alsup explained that, without reaching the other elements of the claim, "imposing a twenty cent fee does not, as a matter of law, make performance under the contract more costly or burdensome. A reasonable person would not think that a twenty cent charge plausibly increased the cost of plaintiff Field's performance under his mobile phone contract."[18]

Where an interference claim is premised on the contents of information posted on a website, a plaintiff must establish that the contents alleged are actionable facts and not merely protected opinion.[19]

In some states, such as Texas, a defendant also may be able to defend an interference claim based on the affirmative defense of justification, which may be based on the exercise of a "good-faith claim to a colorable legal right, even though that claim ultimately proves to be mistaken."[20]

Interference and other state law causes of action poten-

---

[16]*See, e.g., Georgia-Pacific Consumer Products LP v. Myers Supply, Inc.*, 621 F.3d 771 (8th Cir. 2010) (affirming entry of judgment for the defendant under Arkansas law in a tortious interference case based on the absence of evidence that the defendant's conduct was unfair or unreasonable and the "strong presumption that interference with an at-will contract is not improper."); Restatement (Second) of Torts § 768 (1979) (providing that interference with a contract that is terminable at will is less likely to be improper).

[17]*Fields v. Wise Media, LLC*, No. C 12-05160 WHA, 2013 WL 5340490 (N.D. Cal. Sept. 24, 2013).

[18]*Fields v. Wise Media, LLC*, No. C 12-05160 WHA, 2013 WL 5340490, at *5 (N.D. Cal. Sept. 24, 2013).

[19]*See Seaton v. TripAdvisor LLC*, 728 F.3d 592, 603 (6th Cir. 2013) (affirming dismissal of a claim under Tennessee law based on TripAdvisor's inclusion of plaintiff's hotel in its list of "2011 Dirtiest Hotels"). *TripAdvisor* did not involve screenscraping. Rather, it involved unwanted attention on a third party's website.

[20]*WickFire, L.L.C. v. Woodruff*, 989 F.3d 343, 358-59 (5th Cir. 2021) (citations omitted) (affirming a jury verdict of interference in a case involving alleged click fraud, despite substantial evidence supporting WickFire's

tially may be preempted by the Copyright Act unless the plaintiff can plausibly allege an extra element beyond merely copying (such as interference).[21] Claims asserted against websites or other intermediaries for merely republishing third party content or hosting third party material or advertisements likewise may be preempted by the Good Samaritan Exemption to the Telecommunications Act of 1996 (often referred to as the CDA), 47 U.S.C.A. § 230(c).[22]

Where it is not possible for a third party to market a circumvention or screen scraping product without actually accessing an owner's database or website and assenting to its user agreement, the database owner also may be able to sue directly for breach of contract (and potentially other claims based on trespass,[23] conversion,[24] or the Computer Fraud and Abuse Act).[25]

5.03[6] Unjust Enrichment

Where contract remedies may be unavailable, database owners have sought to assert claims against screen scrapers for unjust enrichment.[1] While the elements of a claim may vary from state to state, in general a plaintiff must show

---

defense, including evidence that Google investigated defendants' bidding practices and did not notify WickFire of any problems and even recommended that third parties work with WickFire).

[21]*See supra* § 4.18[1] (copyright preemption in general); *infra* § 5.04 (misappropriation and copyright preemption).

[22]*See, e.g., e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008); *Whitney Information Network, Inc. v. Verio, Inc.*, 79 U.S.P.Q.2d 1606, 2006 WL 66724 (M.D. Fla. Jan. 11, 2006); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1118 (W.D. Wash. 2004) (no liability where images on *Amazon.com* had been provided by a vendor on its zShops platform); *Novak v. Overture Services, Inc.*, 309 F. Supp. 2d 446, 452–53 (E.D.N.Y. 2004) (dismissing the pro se plaintiff's tortious interference claim based on alleged search result manipulation); *Schneider v. Amazon.com, Inc.*, 108 Wash. App. 454, 31 P.3d 37 (Div. 1 2001) (business expectancy); *see generally infra* § 37.05 (analyzing the scope of preemption). Causes of action based on federal copyright and trademark infringement, as well as certain other IP claims, are excluded from the scope of preemption. *See infra* § 37.05[5][B]. The exemption likewise does not exonerate a party for its own conduct. *See infra* § 37.05.

[23]*See infra* § 5.05[1].

[24]*See infra* § 5.05[2].

[25]*See infra* § 5.06.

[Section 5.03[6]]

[1]*See, e.g., Information Handling Services, Inc. v. LRP Publications,*

that (1) defendants were enriched; (2) at plaintiffs' expense; and (3) it is against equity and good conscience to permit defendants to retain what is sought to be recovered.[2] For example, Virginia law requires a plaintiff to show that (1) it conferred a benefit on the defendant, (2) the defendant knew of the benefit and should reasonably have expected to repay the plaintiff, and (3) the defendant accepted or retained the benefit without paying for its value.[3] Similarly, Florida law required a showing that (1) the plaintiff conferred a benefit on the defendant, (2) the defendant had knowledge of the benefit, (3) the defendant accepted or retained the benefit conferred, and (4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying for it.[4] Unjust enrichment is an equitable remedy that will "effect a 'contract implied in law' " to require a party "who accepts and receives the services of another to make reasonable compensation for those services."[5]

Not all states recognize a separate cause of action for unjust enrichment, however. For example, a separate claim for unjust enrichment may not be asserted under California law.[6]

To the extent a claim for unjust enrichment merely seeks

Inc., No. CIV. A. 00-1859, Copy. L. Rep. (CCH) P28,177, 2000 WL 1468535 (E.D. Pa. Sept. 20, 2000) (denying motion to dismiss a claim for unjust enrichment in a database copying case).

[2]*E.g., Estate of Goth v. Tremble*, 59 A.D.3d 839, 873 N.Y.S.2d 364, 367 (3d Dep't 2009) (applying New York law).

[3]*Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 166 (4th Cir. 2012) (Virginia law).

[4]*Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012) (holding that plaintiffs stated a claim for unjust enrichment in a case arising out of a security breach).

[5]*E.g.*, *Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 165 (4th Cir. 2012) (Virginia law; quoting other cases).

[6]*See Hill v. Roll Int'l Corp.*, 195 Cal. App. 4th 1295, 1307, 128 Cal. Rptr. 3d 109 (2011) (holding that "[u]njust enrichment is not a cause of action, just a restitution claim."); *see also, e.g.*, *Astiana v. Hain Celestial Group, Inc.*, 783 F.3d 753, 762 (9th Cir. 2015) (explaining that in California, there is no standalone cause of action for unjust enrichment, which is synonymous with restitution); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for unjust enrichment because such a claim is not viable under California law); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1075-76 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for unjust enrichment based on *Hill v. Roll Int'l Corp.*); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 814–15 (N.D. Cal. 2011) (dismissing a claim for unjust

recovery for unauthorized copying without an extra element, however, the claim will be deemed preempted by the Copyright Act.[7] Similarly, unjust enrichment claims asserted against websites or other intermediaries for merely republishing third party content or hosting third party material such as database content may be preempted by the CDA, 47 U.S.C.A. § 230(c).[8] The CDA, however, does not insulate an interactive computer service provider or user for their own content.

5.04 Common Law Misappropriation and Unfair Competition

Database owners may have claims against parties that scrape material from their websites based on common law misappropriation or unfair competition, to the extent those claims are not preempted by the Copyright Act or, in specific circumstances, the Patent Act, the Uniform Trade Secrets Act or the Communications Decency Act. Those issues are addressed in the following subsections.

5.04[1] Misappropriation (including the "Hot News" Doctrine)

Limited protection for databases may be available under the common law doctrine of misappropriation, to the extent not preempted by the Copyright Act, where an extra element such as breach of fiduciary duty is alleged. Many misappro-

---

enrichment in light of *Hill v. Roll Int'l Corp.,* "[n]otwithstanding earlier cases suggesting the existence of a separate, stand-alone cause of action for unjust enrichment . . . ."); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963, at *15 (N.D. Cal. Sept. 20, 2011) (dismissing plaintiff's claim for unjust enrichment, finding there is no longer any such cognizable claim under California law).

[7] *See, e.g., BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 618 (S.D.N.Y. 2010); *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 680–81 (N.D. Ohio 2010) (holding plaintiff's unjust enrichment claim preempted where it was based on the allegation that defendants took information). *But see Perfect 10, Inc. v. Google, Inc.*, No. CV04-9484, 2008 WL 4217837, at *9 (C.D. Cal. July 6, 2008) (holding plaintiff's unjust enrichment claim not preempted where the claim was premised on right of publicity and trademark violations); *see generally supra* § 4.18[1] (analyzing copyright preemption).

[8] *See, e.g., Ascentive, LLC v. Opinion Corp.*, 842 F. Supp. 2d 450 (E.D.N.Y. 2011); *Rosetta Stone Ltd. v. Google Inc.*, 732 F. Supp. 2d 628 (E.D. Va. 2010) (holding plaintiff's unjust enrichment claim preempted by the CDA), *aff'd in relevant part on other grounds,* 676 F.3d 144, 165–66 (4th Cir. 2012); *see generally infra* § 37.05 (analyzing CDA preemption).

priation claims brought over database copying are premised on the "hot news" doctrine, which makes potentially actionable misappropriation of material that is valuable for its timeliness (such as breaking news stories, stock tips or celebrity news photos), where the copying involves free-riding by a competitor and a threat to the very existence of the product or service supplied by the plaintiff. While a number of courts have recognized and applied the hot news doctrine based on common law misappropriation, as outlined below, others have declined to do so[1] or have sought to avoid a decision on the merits.[2]

In *International News Service v. Associated Press*,[3] a 1918 U.S. Supreme Court decision, the defendant copied AP stories from bulletin boards and early editions of East Coast newspapers and then transmitted and sold paraphrased versions of these stories to newspapers on the West Coast. Although not entitled to copyright protection, the Supreme Court held that breaking news was the "quasi property" of a news-gathering operation and copying this information constituted common law misappropriation.[4]

The Court, in *International News Service*, emphasized that

[Section 5.04[1]]

[1]*See, e.g.*, *Allure Jewelers, Inc. v. Ulu*, No. 1:12CV91, 2012 WL 4322519, at *3 (S.D. Ohio Sept. 20, 2012) (declining to recognize a "hot news" exception under Ohio law for a jeweler's posting of recent information on the price of precious metals in an eBay advertisement for fine jewelry); *Brainard v. Vassar*, 561 F. Supp. 2d 922, 932 (M.D. Tenn. 2008) (noting that "plaintiffs have cited no case law indicating that the Tennessee courts have adopted New York's 'hot-news' causes of action" but ultimately holding that the hot news doctrine did not apply to the case and that plaintiffs' claim for common law misappropriation based on appropriation of a song title preempted by the Copyright Act); *Ultra–Precision Mfg., Ltd. v. Ford Motor Co.,* 01–70302, 2002 WL 32878308, at *4 (E.D. Mich. May 31, 2002) (finding no support for a cause of action for commercial misappropriation under Michigan law).

[2]*See, e.g.*, *DBW Partners, LLC v. Bloomberg, L.P.*, Civil Action No. 19-311 (RBW), 2019 WL 5892489 (D.D.C. Nov. 12, 2019) (dismissing plaintiff's claim for direct and contributory copyright infringement based on alleged copying of Capitol Forum, an investigative news and legal analysis report, and accordingly declining to exercise supplemental jurisdiction over its hot news misappropriation claim, where the issue of whether D.C. should adopt hot news misappropriation was best addressed in the D.C. Superior Court, rather than federal court).

[3]*International News Service v. Associated Press*, 248 U.S. 215 (1918).

[4]Federal common law subsequently was abolished by *Erie R. Co. v. Tompkins*, 304 U.S. 64 (1938). As discussed below, the general common

newsgathering carried with it "the expenditure of labor, skill, and money" and that when another party appropriates breaking news, it "is endeavoring to reap what it has not sown."[5]

Since the time the Court decided *International News Service*, the Copyright Act was amended to expressly preempt state remedies equivalent to those protected by the Copyright Act.[6] A common law misappropriation claim will be preempted if it lacks an "extra element" necessary to support an independent claim.[7] A claim for common law misappropriation based on copying therefore will be limited to circumstances such as where a confidential relationship may be shown or where there was some other breach of trust or agreement or passing off[8] or misappropriation under the hot news doctrine.[9]

In *National Basketball Association v. Motorola, Inc.*,[10] the Second Circuit explained *International News Service* as a "hot news" case, which has continuing validity under New York state law to the extent it is limited to its particular facts (one wire service taking advantage of a time delay to profit from the other company's collection of current news stories). The Second Circuit held that a claim for common

---

law principles of misappropriation in breaking news cases articulated in International News remain valid under state common law, to the extent not preempted by the Copyright Act.

[5]*International News Service v. Associated Press*, 248 U.S. 215, 239–40 (1918).

[6]*See* 17 U.S.C.A. § 301.

[7]*E.g., Kregos v. Associated Press*, 3 F.3d 656, 666 (2d Cir. 1993); *Summit Mach. Tool Mfg. Corp. v. Victor CNC Systems, Inc.*, 7 F.3d 1434, 1441–42 (9th Cir. 1993); *Quadrille Wallpapers and Fabric, Inc. v. Pucci*, No.1:10-CV-1394, 2011 WL 3794238, at *9 (N.D.N.Y. Aug. 24, 2011) (finding that plaintiff's unfair competition and misappropriation claims were not preempted because the bases of both claims under state law required an additional element of a breach of confidential relationship); *see generally supra* § 4.18[1] (copyright preemption).

[8]*See, e.g., Cable Vision, Inc. v. KUTV, Inc.*, 335 F.2d 348, 352 (9th Cir. 1964) (International News was premised on a theory of "passing off."), *cert. denied*, 379 U.S. 989 (1965).

[9]*See Financial Information, Inc. v. Moody's Investors Service, Inc.*, 808 F.2d 204, 209 (2d Cir. 1986) (explaining that hot news misappropriation is "a branch of the unfair competition doctrine, not preempted by the Copyright Act according to the House Report.").

[10]*National Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841 (2d Cir. 1997).

law misappropriation, although not established in that case, may be asserted, and will not be preempted, where (1) a plaintiff generates or gathers information at a cost, (2) the information is time-sensitive, (3) a defendant's use of the information constitutes free-riding on the plaintiff's efforts, (4) the defendant is in direct competition with a product or service offered by plaintiff, and (5) the ability of other parties to free-ride on the efforts of the plaintiff or others would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened.

Although the Second Circuit in *Motorola* reversed the injunction that had been issued by the lower court based on its determination that the plaintiff could not make out a claim for hot news misappropriation, an increasing number of Internet-related suits have been brought over the years (particularly in New York and California) relying on *Motorola* for both its preemption analysis and description of the elements required to state a claim for common law misappropriation under New York law in a case involving "hot news." In 2011, however, a later Second Circuit panel potentially narrowed its reach—at least as interpreted in some subsequent lower court decisions—and the majority disavowed *Motorola*'s five-part test as *dicta* not necessary to the court's holding in that case.

In *Barclays Capital, Inc. v. TheFlyOnTheWall.com*,[11] Judge Sack (writing for himself and Judge Pooler, in a case where Judge Raggi filed a concurring opinion) emphasized that the scope of the preemption exception was "narrow," cautioning that "[t]he broader the exemption, the greater the likelihood that protection of works within the 'general scope' of the copyright and the type of works protected by the Act will receive disparate treatment depending on where the alleged tort occurs and which state's law is found to be applicable."[12] The majority also rejected the "moral dimension" to hot news misappropriation cases, concluding that "unfairness alone is immaterial to a determination whether a cause of action for misappropriation has been preempted by the Copyright

[11] *Barclays Capital Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876 (2d Cir. 2011).

[12] *Barclays Capital Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876, 897 (2d Cir. 2011).

Act."[13] The majority instead applied the traditional three-part test for evaluating copyright preemption, evaluating (1) whether a claim seeks to vindicate "legal or equitable rights that are equivalent" to one of the bundle of exclusive rights already protected by copyright law under 17 U.S.C.A. § 106 (reproduction, distribution, public performance, public display and the right to make derivative works),[14] (2) whether the work in question falls within the ambit of copyright protection (which may include both protectable and uncopyrightable works) and (3) if an "extra element" is "required instead of or in addition to the acts of reproduction, performance, distribution or display, in order to constitute a state-created cause of action . . . ."[15] Based on this test, the Second Circuit reversed the entry of judgment for the plaintiffs, finding their claims preempted. Judge Raggi concurred, although she would have applied the five-part *Motorola* test rejected by the other judges based on her conclusion that it was not mere *dictum*. In her view, the plaintiffs failed to satisfy the "direct competition" requirement of the *Motorola* test.[16]

In *Fox News Network, LLC v. TVEyes, Inc.*,[17] Judge Alvin K. Hellerstein of the Southern District of New York followed *Barclays* in holding that a news network's hot news misappropriation claim against a service that recorded all television and radio broadcasts for more than 1,400 stations, 24 hours a day, every day, and transformed this material into a searchable database for its paying subscribers, which included the White House, more than 100 members of

---

[13]*Barclays Capital Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876, 896 (2d Cir. 2011). The majority noted that:

> The adoption of new technology that injures or destroys present business models is commonplace. Whether fair or not, that cannot, without more, be prevented by application of the misappropriation tort. Indeed, because the Copyright Act itself provides a remedy for wrongful copying, such unfairness may be seen as supporting a finding that the Act preempts the tort.

Id.

[14]*See supra* § 4.04[1].

[15]*Barclays Capital Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876, 892–907 (2d Cir. 2011), *quoting in part Computer Associates Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 716 (2d Cir. 1992) (quoting Nimmer on Copyright § 1.01[B], at 1-14-15 (1991)).

[16]The *FlyInTheWall* case is discussed in greater detail later in this section.

[17]*Fox News Network, LLC v. TVEyes, Inc.*, 43 F. Supp. 3d 379 (S.D.N.Y. 2014).

Congress and ABC Television, was preempted because Fox's claim did not include an extra element besides copying. In that case, TVEyes offered paying business subscribers an indexing and clipping service that allowed them to search for and find video excerpts for purposes such as evaluating and criticizing broadcast journalism, tracking and correcting misinformation, evaluating commercial advertising, evaluating national security risks, and tracking compliance with financial market regulations. In holding Fox's claim preempted, Judge Hellerstein explained that "TVEyes is not a valuable service because its subscribers credit it as a reliable news outlet, it is valuable because it reports what the news outlets and commentators are saying and therefore does not 'scoop' or free-ride on the news services."[18]

Courts previously had allowed hot news misappropriation claims to proceed based on *Motorola* in a number of Internet cases. In *Pollstar v. Gigmania Ltd.*,[19] for example, a federal district court in California denied the defendant's motion to dismiss, allowing plaintiff's suit for misappropriation (and unfair competition based on palming off) to proceed. In that case, the plaintiff had provided access to a database it created that included current concert information, subject to posted terms and conditions. The court rejected the defendant's arguments that plaintiff's misappropriation and unfair competition claims were preempted by the Copyright Act, holding that the plaintiff had sufficiently pled a "hot news" claim.

Similarly, in *Facebook, Inc. v. ConnectU LLC*,[20] the court found that Facebook's misappropriation claim against a competitor was not preempted where the competitor collected the email addresses of Facebook's registered users, posted them on its website and then sent unsolicited commercial email to those users. The court found that the email addresses were not works of authorship or otherwise protectable under the copyright Act and that the defendant "had not shown that it was alleged to have misappropriated

---

[18]*Fox News Network, LLC v. TVEyes, Inc.*, 43 F. Supp. 3d 379, 399 (S.D.N.Y. 2014). This particular ruling was not challenged on appeal. *See Fox News Network, LLC v. TVEyes, Inc.*, 883 F.3d 169, 174 n.2 (2d Cir. 2018).

[19]*Pollstar v. Gigmania, Ltd.*, 170 F. Supp. 2d 974 (E.D. Cal. 2000).

[20]*Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087 (N.D. Cal. 2007).

uncopyrightable 'elements' of a work of authorship otherwise within the scope of the Copyright Act."[21]

In *Weingand v. Harland Financial Solutions, Inc.*,[22] the court similarly found plaintiff's unjust enrichment claim not preempted because the material at issue was confidential data such as social security numbers, addresses, and bank account information, and thus not copyrightable, and the plaintiff alleged the additional element of a contractual relationship.

In *Chicago Board Options Exchange, Inc. v. International Securities Exchange, LLC*,[23] an intermediate appellate court in Illinois affirmed the entry of summary judgment in favor of the plaintiffs, a national securities exchange and index providers, on their claim for common law misappropriation against a competing securities exchange, which had announced its intention to offer index options based on stock indices, without obtaining a license. The court held that plaintiffs' claim was not preempted because it was premised on unlicensed use of plaintiff's ideas, systems, and concepts, which are not entitled to copyright protection—namely unauthorized use of the research, expertise, reputation and goodwill associated with plaintiff's product. The court also held that the defendant's proposed use of the index for its own financial products constituted common law misappropriation under Illinois law.

A court in California likewise held that celebrity news site X17 stated a claim for hot news misappropriation against blogger Perez Hilton for pervasive copying of its paparazzi photographs,[24] although Hilton defeated a motion for a preliminary injunction in a similar suit brought in New York for copying facts from another website where the court found that the information allegedly copied was widely available over the Internet (usually before it had been posted on the plaintiff's own website) and the plaintiff had not shown that

---

[21]*Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087, 1092–93 (N.D. Cal. 2007).

[22]*Weingand v. Harland Financial Solutions, Inc.*, No. C-11-3109 EMC, 2012 WL 2327660, at *7 (N.D. Cal. June 19, 2012).

[23]*Chicago Board Options Exchange, Inc. v. International Securities Exchange, LLC*, 973 N.E.2d 390 (Ill. App. 2012).

[24]*See X17, Inc. v. Lavandeira*, 563 F. Supp. 2d 1102 (C.D. Cal. 2007).

she had incurred significant costs compiling it.[25] In the California action, the court found that X17 stated a claim where it alleged that: (1) it expended substantial costs and resources to gather, obtain, and create the photographs that Lavandeira (Perez Hilton) disseminated; (2) the photographs were time-sensitive; (3) the parties were direct competitors; (4) Lavandeira was earning revenue by free-riding on the substantial hard work of X17; (5) if the activities continued, they would remove X17's incentive to gather celebrity news photographs and threaten the continued existence of its business; and (6) Lavandeira's activities had substantially harmed X17.[26]

In so ruling, Judge Feess rejected the defendant's argument that a hot news claim was limited to factual information. He held that a claim could be based on photographs, noting that the medium was not important in either *International News Service* or *Motorola*. The court also observed in *dicta* that misappropriation claims were not limited to "hot news" so long as an extra element beyond copying was alleged (so that the claim would not be preempted). Among other things, Judge Feess noted that misappropriation claims could be based on breach of a fiduciary duty, in addition to hot news.

In *Associated Press v. All Headline News Corp.*,[27] a court in the Southern District of New York denied the defendant's motion to dismiss a claim for misappropriation of "hot" or "breaking news," where the plaintiff alleged each of the *NBA v. Motorola* elements in connection with defendant's operation of All Headline News Corp. (AHN), an Internet site that does not undertake any original reporting and allegedly hired poorly paid individuals to find news stories on the

---

[25]*See Silver v. Lavandeira*, No. 08 Civ. 6522(JSR)(DF), 2009 WL 513031 (S.D.N.Y. Feb. 26, 2009) (denying plaintiff's motion for a preliminary injunction because the plaintiff was unlikely to prevail on copyright infringement, DMCA and hot news misappropriation claims).

[26]*See X17, Inc. v. Lavandeira*, 563 F. Supp. 2d 1102, 1108–09 (C.D. Cal. 2007). The court was ruling on a motion to dismiss. Judge Feess emphasized that "[w]hether or not X17 can prove its case is a matter that the Court does not address in this ruling. The Court concludes only that X17 has adequately pled the . . . elements required to state a claim for California's misappropriation tort . . ." and the additional elements to come within the sub-set of misappropriation claims based on hot news. *Id.* at 1108.

[27]*Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454 (S.D.N.Y. 2009).

Internet (including AP stories) and prepare them for republication as AHN stories by either rewriting the articles or copying the stories in full. Plaintiffs alleged that, among other things, defendants copied AP's breaking news stories and reproduced them as stories that originated with AHN.[28]

The court also denied defendants' motion to dismiss AP's state law unfair competition claim, finding that the plaintiff had stated a claim for passing off by alleging that AHN passed off AP content as its own.[29] Neither plaintiff's "hot news" nor its passing off claims were found preempted.[30]

In a subsequent case also from the Southern District of New York, *BanxCorp. v. Costco Wholesale Corp.*,[31] a hot news

---

[28]*Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454, 461 (S.D.N.Y. 2009). *All Headline News* was decided prior to the Second Circuit's decision in *Barclays Capital Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876 (2d Cir. 2011), which narrowly construed the scope of "hot news" claims of common law misappropriation that could survive copyright preemption. Nevertheless, as discussed later in this section, the majority cited *All Headline News* approvingly as a case closer to the facts of *International News Service* than the one it was deciding.

[29]*Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454, 464 (S.D.N.Y. 2009). The court also ruled that the Associated Press could state a DMCA claim for removal of copyright management information (*see infra* § 5.07[2]), but dismissed certain Lanham Act claims, holding that defendant's use of the trademarked term "AP" or "Associated Press" in connection with phrases such as "According to an AP report," to attribute certain facts to the Associated Press, did not constitute trademark infringement, that the defendant's characterization of itself as a "news service" or news-gathering organization did not constitute false designation of origin, and that defendants did not make false or misleading representations to consumers by editing news stories to omit the creators of original source material when paraphrasing them, but citing them directly by name when quoting them.

[30]Prior to *Barclay's*, courts had almost universally held that hot news claims that incorporate the elements set forth in *Motorola* are not preempted by the Copyright Act. In *Lowry's Reports, Inc. v. Legg Mason, Inc.*, 271 F. Supp. 2d 737, 754–57 (D. Md. 2003), however, the court, citing law review articles, held that the plaintiff's hot news claim in that case was preempted. The court found that allegations such as "free riding" were equivalent to copyright claims and did not amount to an extra element. The court's cursory analysis in *Legg* has not been followed by other courts and has been criticized. *See X17, Inc. v. Lavandeira*, 563 F. Supp. 2d 1102, 1106 (C.D. Cal. 2007) (rejecting *Legg* as unpersuasive and inconsistent with the legislative history of the Copyright Act).

[31]*BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 611–18 (S.D.N.Y. 2010). *BanxCorp.* was decided prior to the Second Circuit's decision in *Barclays Capital Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876 (2d

claim based on the allegation that 100% of a continuously updated database, including at least some hot news, was misappropriated by a defendant that allegedly exceeded the scope of its license agreement, likewise was held not to be preempted. The court, in ruling on the defendant's motion to dismiss, held that claims for misappropriation based on hot news and breach of a license agreement, as alleged, were not preempted, but claims for unfair competition and unjust enrichment were preempted.

"Hot news" misappropriation generally has been easier to allege than prove and most Internet cases to date have been resolved through motion practice or settlement. In the one case to proceed to judgment, *Barclays Capital, Inc. v. TheFlyOnTheWall.com*,[32] the trial court had entered judgment for the plaintiffs following a bench trial based on common law misappropriation of time-sensitive stock recommendations (in addition to copyright infringement), but the judgment was reversed on appeal by the Second Circuit, which remanded the case with instructions to dismiss plaintiffs' claim as preempted by the Copyright Act. The defendant in that case did not appeal the court's judgment and entry of an injunction under the Copyright Act.

In *TheFlyOnTheWall*, plaintiffs Barclay's Capital, Merrill Lynch and Morgan Stanley, sued the defendant for unauthorized dissemination of its company analysis and recommendations, which were primarily valuable (to potential investors seeking to buy or sell stocks at a profit) for their timeliness, often overnight before the market opened. Initially, TheFlyOnTheWall.com disseminated plaintiff's copyrighted reports verbatim, but after receiving a cease and desist letter from the plaintiffs, changed its practices to simply disseminate headlines (such as "EQIX: Equinox initiated with a Buy at Bofa/Merrill. Target $110")—typically around 600 per day—drawn from sixty-five investment firms' research analysts, including the three plaintiff firms. Over time, it diversified its news sources. Whereas recommendations from plaintiffs' firms accounted for 7 percent of its newsfeed in 2005, by 2009 they represented only approximately 2.5 percent. The defendant's sources for the in-

---

Cir. 2011), which narrowly construed the scope of copyright preemption for "hot news" claims of common law misappropriation.

[32]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

formation from plaintiffs also changed over time. Initially, TheFlyOnTheWall relied entirely on employees of plaintiffs' firms, who transmitted the reports to it directly (without authorization), allowing the defendant to disseminate the information to its own subscribers before the opening of the market. As a result of the litigation, the defendant claimed to have stopped looking at plaintiffs' reports directly and instead relied on information received from independent sources, confirming reports from two or three independent sources before publishing them.

In holding the defendant liable for hot news misappropriation, the trial court had rejected the argument that by obtaining plaintiffs' recommendations from sources other than plaintiffs, it was obtaining information that was already "public" and therefore could be freely republished.

District Court Judge Cote had analyzed the *Motorola* factors, finding that they all supported liability. First, with respect to the cost of information, the district court found that plaintiffs collectively employed hundreds of skilled analysts and spent hundreds of millions of dollars each year to product their equity research reports.

Second, the district court had held that plaintiffs showed that the value of the information generated or collected by them was highly time-sensitive. The value of stock tips, the court ruled, was in disseminating them while they were "fresh." Judge Cote found that plaintiffs' clients used the analysts' opinions "to execute trades in anticipation of stock price movement in order to capture the maximum benefit from the movement." To reap the greatest benefit from their research reports through commission income, the court wrote that the plaintiffs had to engage "in a costly, frenzied process to try to be the first to inform their clients" of their recommendations.[33] District Court Judge Cote also found that the defendant's own conduct verified the time-sensitive nature of the data by emphasizing this fact to its own subscribers and business partners and by suing one of its own competitors for hot news misappropriation and alleging that the value of its newsfeeds was highly time sensitive.

Third, the trial court held that the defendant's use of plaintiff's information constituted free-riding on the plain-

[33] *Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 336 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

tiff's costly efforts to generate or collect it (or the diversion of value from a business rival's efforts without payment). The defendant did no research of its own, allowing it to sell plaintiffs' recommendations at a cut-rate price. Although the defendant provided attribution for the recommendations it relayed to its subscribers and business partners, Judge Cote wrote that this fact merely "underscore[d] its pilfering."[34] The trial court was unimpressed with defendant's argument that many others in the industry did the same, writing that "[t]he fact that others also engage in unlawful behavior does not excuse a party's own illegal conduct."[35]

The defendant had argued that because it no longer received plaintiffs' information directly from plaintiffs, but instead from third parties, it was merely disseminating information that was already in the marketplace. The trial court, however, explained that the legally salient fact was not that lawful subscribers repeat news to their friends or colleagues, which is permissible, it is that plaintiffs systematically gathered plaintiffs' recommendations (even if indirectly from third parties) and then used it to run a profitable business dedicated to systematically gathering and selling plaintiffs' recommendations.[36]

The trial court had also rejected defendant's argument that its reports included "much more" than merely plaintiffs' recommendations, noting that liability may be imposed even where misappropriation only relates to a small part of a defendant's business (as was the case in *International News Service*).

Fourth, the trial court found that the defendant was a direct competitor of plaintiffs in the area of plaintiffs' "primary business." The defendant also was found to have taken steps to compete even more directly by aligning itself with discount brokerage houses that could execute trades. Judge Cote also noted that the defendant previously had asserted a counterclaim for unfair competition against the plaintiffs.

Fifth, the trial court found that the defendant's ability to freeride on plaintiffs' efforts could so reduce the incentive to

---

[34]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

[35]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 337 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

[36]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 338 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

produce the reports that their existence or quality were substantially threatened absent injunctive relief. Plaintiffs had shown both significant losses and the risk of continued misappropriation by the defendant

In addition to entering judgment for plaintiffs on their hot news misappropriation claim, the district court entered judgment in their favor on their copyright infringement claim, issuing a permanent injunction and awarding statutory damages, prejudgment interest and attorneys' fees (but only the portion of fees directly and predominantly concerned with the prosecution of plaintiffs' copyright claim, potentially reduced in light of the disparity in resources between the plaintiffs—major investments firms—and the defendant, and defendant's financial condition).[37]

Despite the strong opinion, the injunction actually issued by Judge Cote was narrow. Plaintiffs had sought an injunction against reporting a stock recommendation until the later of four hours after it was released or 12:00 PM Eastern Time. The court, however, only enjoined the defendant from disseminating information from research reports released while the market is closed until the later of thirty minutes after the market closed or 10:00 AM Eastern Time.

Judge Cote also invited the defendant to seek a reevaluation of the order in a year's time if, during that time, plaintiffs did not also take action against defendant's competitors. The trial court observed that since Fly "first built its business around the misappropriation of" plaintiffs' reports and recommendations, the practice of posting this information had "become a widespread phenomenon."[38] Accordingly, Judge Cote wrote that "[i]t would be unjust to restrain Fly from publishing" plaintiffs' recommendations if plaintiffs "were to acquiesce in the unauthorized publication . . . by others . . . ."[39] The trial court held that the defendant could "apply to modify or vacate the injunction" if it could demonstrate that plaintiffs did not "take reasonable steps to re-

---

[37]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 328–31 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011); *see generally supra* §§ 5.02 (copyright protection), 4.14 (copyright damages), 4.15 (attorneys' fees under the Copyright Act).

[38]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 347 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

[39]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 347 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

strain the systematic, unauthorized misappropriation of their Recommendations, for instance, through the initiation of litigation against any parties with whom negotiation proves unsuccessful."[40]

In reversing the judgment for the defendant on plaintiffs' claim for common law misappropriation, the majority of the Second Circuit panel that considered the case (as noted earlier) rejected the five-part *Motorola* test as based on *dicta,* but purported to apply *Motorola*'s actual holding. Noting that it was not determinative for preemption purposes that the facts contained in plaintiffs' recommendations were not entitled to copyright protection, the majority found that the reports and recommendations fell within the "general scope" of the Copyright Act. The majority took issue with the use of the term "free riding" in hot news jurisprudence, noting that in *International News Service*, as underscored in *Motorola*, free riding involved taking material from a plaintiff and selling it as the defendant's own. Applying this narrower understanding of free riding to plaintiffs' recommendations—the conclusions contained in reports on whether to buy or sell a stock and what the target value should be—the majority concluded that TheFlyOnTheWall was very different from the defendant in *International News Service*. The majority underscored that the plaintiffs' recommendations were "*create[d]*using their expertise and experience, rather than *acquire[d]* through efforts akin to reporting."[41] In the majority's view, "[t]he Firms are making the news; Fly, despite the Firms' understandable desire to protect their business model, is breaking it."[42] In addition, the majority emphasized that TheFlyOnTheWall was not selling the recommendations as its own, which further distinguished the case from *International News Service*.

The majority also found significant the fact that the Supreme Court in *International News Service* referred to the defendant's tortious behavior as "amount[ing] to an unauthorized interference with the normal operation of complainant's business *precisely at the point where the profit is to be*

---

[40]*Barclays Capital Inc. v. Theflyonthewall.com*, 700 F. Supp. 2d 310, 347–48 (S.D.N.Y. 2010), *rev'd in part*, 650 F.3d 876 (2d Cir. 2011).

[41]*Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 903 (S.D.N.Y. 2011)(emphasis in original).

[42]*Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 902 (S.D.N.Y. 2011).

reaped, in order to *divert a material portion of the profit* from those who have earned it to those who have not . . . ."[43] By contrast, although the majority conceded that the plaintiffs would likely earn more revenue if their recommendations were not disseminated by third parties and that there was some evidence that TheFlyOnTheWall had linked some of its own subscribers to competing discount brokerage services, the majority did not view its publication of the recommendations as "an unauthorized interference with the normal operations of [plaintiffs'] legitimate business precisely at the point where the profit is to be reaped . . . ."[44]

Judge Reena Raggi, concurring, would have applied the *Motorola* test, finding it binding (and not *dictum*), but concurred based on her conclusion that direct competition could not be shown. Like the majority, she premised her opinion on the fact that the defendant produced an aggregate product reporting recommendations from many different firms, among other financial news, attributing each recommendation to its source. The majority, she wrote, drew "a bright line distinguishing between the Firms, who generate news, and Fly and other news aggregators, who 'break' the news, with the former falling outside of hot-news protection."[45] By contrast, she wrote that she was "not prepared to foreclose the possibility of a 'hot-news' claim by a party who disseminates news it happens to create."[46] Instead, she concluded that plaintiffs could not state a non-preempted claim because plaintiffs and defendant were not direct competitors. *Motorola,* she explained, involved the "plaintiff's failure to show free riding on and a sufficient threat to its services," but also underscored that "only products in the 'keenest' of competition satisfy the direct competition requirement for a non-preempted claim."[47]

Although the majority disclaimed that it did "not mean to

---

[43] *Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 904 (S.D.N.Y. 2011), *quoting International News Service v. Associated Press*, 248 U.S. 215, 240 (1918) (emphasis added by the Second Circuit).

[44] *Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 904–05 (S.D.N.Y. 2011).

[45] *Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 913 (S.D.N.Y. 2011) (Raggi, J., concurring).

[46] *Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 913 (S.D.N.Y. 2011) (Raggi, J., concurring).

[47] *Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 913 (S.D.N.Y. 2011) (Raggi, J., concurring), *quoting International News Service*

be parsing the language of *INS* as though it were a statement of law the applicability of which determines the outcome of this appeal"[48] the majority, in fact, applied *International News Service* very narrowly to its literal facts, ascribing as *dicta* broader notions of "free riding" that were seemingly approved-of by the Second Circuit panel in *Motorola*. The net effect, at least in the Second Circuit, is to scale back the circumstances under which a claim of hot news misappropriation may be brought to circumstances where a competitor takes valuable data and seeks to sell it as its own under circumstances akin to *International News Service*.[49]

Even if otherwise viable, misappropriation claims may be preempted by the Uniform Trade Secrets Act (where enacted), which provides that the Act "displaces conflicting tort, restitutionary, and other law of this State pertaining to civil liability for misappropriation of a trade secret."[50] Section 7 has been construed in some (but not all) jurisdictions to preempt claims premised on the wrongful taking and use of confidential business and proprietary information, regard-

---

v. Associated Press, 248 U.S. 215, 221 (1918).

[48]*Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 905 (S.D.N.Y. 2011).

[49]Despite its characterization of much of the *Motorola* decision as *dicta*, the majority speculated that "[i]f a Firm were to collect and disseminate to some portion of the public facts about securities recommendations in the brokerage industry (including, perhaps, such facts it generated itself—its own Recommendations), and were Fly to copy the facts contained in the Firm's hypothetical service, it might be liable to the Firm on a 'hot-news' misappropriation theory." *Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 905–06 (S.D.N.Y. 2011).

The Second Circuit majority also cited approvingly *Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454 (S.D.N.Y. 2009), which was discussed earlier in this section, as a case "presenting facts more closely analogous to INS . . . ." *Barclays Capital Inc. v. Theflyonthewall.com*, 650 F.3d 876, 906 (S.D.N.Y. 2011). On the other hand, the fact that in *All Headline News* the parties had argued over choice of law, assuming that a hot news claim under New York law would not be viable if Florida law were to have been applied, was cited by the majority as a reason why the doctrine should be narrowly construed to promote greater uniformity, rather than the "sort of patchwork protection that the drafters of Copyright Act preemption provisions sought to minimize . . . ." *Id.* at 897–98.

[50]UTSA § 7; *infra* § 10.17 (analyzing case law on UTSA preemption). A copy of the UTSA is reprinted in the appendix to chapter 10.

less of whether the information constitutes a trade secret.[51] Claims against interactive computer service providers for misappropriation by third parties also may be preempted by the Communications Decency Act.[52]

5.04[2] Unfair Competition

Most states have enacted statutes or recognize common law claims for unfair competition. The heading "unfair competition" may include claims for common law misappropriation,[1] trademark infringement or dilution, passing off or equivalent state law corollaries to the remedies available

---

[51]*See, e.g.*, *Heller v. Cepia, LLC*, No. C 11–01146 JSW, 2012 WL 13572, at *7 (N.D. Cal., Jan. 4, 2012) (dismissing claims for common law misappropriation, conversion, unjust enrichment, and trespass to chattels, because these claims, "premised on the wrongful taking and use of confidential business and proprietary information, regardless of whether such information constitutes trade secrets, are superseded by the CUTSA."); *Glasstech, Inc. v. TGL Tempering Sys., Inc.*, 50 F. Supp. 2d 722, 730 (N.D. Ohio 1999) (holding common law claims for misuse and misappropriation, unfair competition, and unjust enrichment preempted by Ohio's Uniform Trade Secrets Act); *see generally infra* § 10.17 (discussing conflicting lines of cases on whether a claim is preempted even if based on information that may not be protectable as a trade secret).

[52]47 U.S.C.A. § 230(c); *Stevo Design, Inc. v. SBR Mktg. Ltd.*, 919 F. Supp. 2d 1112, 1127 (D. Nev. 2013) (dismissing plaintiffs' complaint for common law misappropriation under Florida law with leave to amend); *infra* § 10.17; *see generally infra* § 37.05 (analyzing the CDA in substantially greater detail).

[Section 5.04[2]]

[1]*See Fox News Network, LLC v. TVEyes, Inc.*, 43 F. Supp. 3d 379, 399–400 (S.D.N.Y. 2014) (holding that a New York state law misappropriation claim, grounded in either deception or appropriation of the exclusive property of a plaintiff, may be maintained in certain circumstances "based on the equitable doctrine that recognizes that 'a person shall not be allowed to enrich himself unjustly at the expense of another.' "; *quoting Georgia Malone & Co. v. Rieder*, 19 N.Y.3d 511, 516, 950 N.Y.S.2d 333, 973 N.E.2d 743 (2012)); *see also Financial Information, Inc. v. Moody's Investors Service, Inc.*, 808 F.2d 204, 209 (2d Cir. 1986) (explaining that hot news misappropriation is "a branch of the unfair competition doctrine, not preempted by the Copyright Act according to the House Report."); *supra* § 5.04[1] (analyzing hot news misappropriation). In *Fox News*, the court held that plaintiff's unfair competition claim, like its claim for hot news misappropriation, was preempted by the Copyright Act. *See Fox News Network, LLC v. TVEyes, Inc.*, 43 F. Supp. 3d 379, 399–400 (S.D.N.Y. 2014) (holding that bad faith or a bad intent did not constitute an extra element); *see generally supra* § 5.04[1] (discussing Fox's hot news claim).

under the federal Lanham Act,[2] and potentially even broader claims based on any action that may be deemed unfair if undertaken by a business or potential competitor. Under California's infamous unfair competition statute, Business & Professions Code § 17200, for example, a plaintiff may sue for "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising . . ." and any act prohibited by California's false advertising statute.[3] Any violation of a state or federal law (including those that do not afford private causes of action) or even a state or federal policy potentially may be actionable under this very broad statute, so long as the plaintiff may show that it has "suffered injury in fact and has lost money or property as a result of such unfair competition."[4] Indeed, "a practice may be deemed unfair even if not specifically proscribed by some other law."[5]

Hence, unfair competition may be a broader, more general claim that can be asserted in a scraping case, even if other claims aren't viable.[6] Where a plaintiff can state a claim for unfair competition it may be able to recover actual or statu-

---

[2]*See infra* § 5.08.

[3]Cal. Bus. & Prof. Code § 17200. The provisions of California's false advertising statute that are also expressly made actionable under section 17200 are codified at Cal. Bus. & Prof. Code §§ 17500 to 17580; *see generally infra* § 6.12[6] (analyzing section 17200 in greater detail).

[4]Cal. Bus. & Prof. Code § 17200. "An injury in fact is '[a]n actual or imminent invasion of a legally protected interest, in contrast to an invasion that is conjectural or hypothetical." *Hall v. Time Inc.*, 158 Cal. App. 4th 847, 853, 70 Cal. Rptr. 3d 466, 470 (4th Dist. 2008).

[5]*Hall v. Time Inc.*, 158 Cal. App. 4th 847, 853, 70 Cal. Rptr. 3d 466, 470 (4th Dist. 2008); *see also, e.g.*, *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 318, 120 Cal. Rptr. 3d 741 (2011) (finding that injury from frustration of patriotic desire to buy fully American-made products where the defendant falsely advertised that products were "Made in U.S.A." was sufficient to satisfy the standing requirement to state a claim under section 17204); *see generally infra* § 6.12[6] (analyzing this statute in greater detail).

[6]*See, e.g.*, *Domain Name Commission Ltd v. DomainTools, LLC*, 449 F. Supp. 3d 1024, 1030-32 (W.D. Wash. 2020) (dismissing plaintiff's CFAA claim for scraping data because plaintiff could not meet the $5,000 damage threshold but holding that plaintiff stated a claim under Washington's Consumer Protection Act ("CPA"), Wash. Rev. Code Ann. § 19.86, where plaintiff alleged that defendant's efforts to circumvent the rate limiting and use restrictions plaintiff imposed to protect the data on its servers was "unfair or deceptive," that defendant engaged in these unfair acts in order to create and sell its products and services, that the public's interest was impacted because consumers are deprived of their privacy, and that

tory damages and/or attorneys' fees. Even where a claim is limited to just equitable relief or restitution (and not damages)—as, for example, under California's section 17200[7]—the assertion of a claim may have settlement value because injunctive relief could impact a company's business model. Of course, to obtain equitable relief, a party must establish the inadequacy of legal remedies such as damages,[8] which may be difficult where the sole harm to a database owner is financial.[9]

Database owners may assert unfair competition claims against those who copy their databases or provide the tools for third parties to do so, provided the claim alleges more than mere copying, which otherwise would be preempted by the Copyright Act[10] (or, less frequently, the Patent Act, which is separately addressed in section 5.04[3]). In *Marobie-Fl, Inc. v. National Association of Fire Equipment Distributors*,[11] for example, a federal court in Chicago entered summary judgment on plaintiff's claim for common law unfair compe-

---

plaintiff had incurred expenses and suffered injury to reputation and good will as a result).

[7]*See, e.g.*, *Thomas v. Kimpton Hotel & Restaurant Group, LLC*, Case No. 19-cv-01860-MMC, 2020 WL 3544984, at *3-4 (N.D. Cal. June 30, 2020) (dismissing plaintiffs' 17200 claim in a putative cybersecurity breach class action suit where plaintiff failed to allege facts sufficient to support either a claim for injunctive relief or a claim for restitution).

[8]*See, e.g.*, *Shay v. Apple Inc.*, Case No.: 20cv1629-GPC(BLM), 2021 WL 1733385 (S.D. Cal. May 3, 2021) (dismissing plaintiff's UCL claim), *citing Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020); *In re California Gasoline Spot Market Antitrust Litigation*, Case No. 20-cv-03131-JSC, 2021 WL 1176645, at *7-8 (N.D. Cal. Mar. 29, 2021) (dismissing plaintiff's UCL claim with leave to amend if plaintiffs had a good faith basis to allege inadequacy of legal remedies).

[9]A different case potentially may be presented if screen scraping poses security or reputational concerns to a company.

[10]17 U.S.C.A. § 301; *Information Handling Services, Inc. v. LRP Publications, Inc.*, No. CIV. A. 00-1859, Copy. L. Rep. (CCH) P28,177, 2000 WL 1468535 (E.D. Pa. Sept. 20, 2000) (holding plaintiff's unfair competition claim to be preempted in a case alleging database copying). *But see BanxCorp v. Costco Wholesale Corp.*, 723 F. Supp. 2d 596, 611–18 (S.D.N.Y. 2010) (holding that claims for breach of a license agreement and misappropriation based on hot news were not preempted in a case alleging that the defendant, a licensee, misused money market and CD data, but claims for unfair competition and unjust enrichment were preempted); *see generally supra* § 4.18[1] (copyright preemption).

[11]*Marobie-FL, Inc. v. National Ass'n of Fire Equipment Distributors*, 983 F. Supp. 1167 (N.D. Ill. 1997).

tition against the owner of a website and its hosting company based on preemption, where the plaintiff had failed to allege likelihood of confusion or facts to support a finding of an "extra element" that "changes 'the nature of the action so it is qualitatively different from a copyright infringement claim'."[12] The court noted in *dicta*, however, that while unfair competition claims premised on "passing off" generally are not barred by the Copyright Act, state law claims based on "reverse passing off" typically are preempted.[13]

State law unfair competition claims brought against interactive computer services or users based on content originating with others may be preempted by the Communications Decency Act (CDA).[14] CDA preemption is analyzed extensively in section 37.05.

Unfair competition claims also potentially may be preempted by the Patent Act. "If a plaintiff bases its tort action on conduct that is protected or governed by federal patent law, then the plaintiff may not invoke the state law remedy, which must be preempted for conflict with federal patent

---

[12]983 F. Supp. at 1167, *quoting Computer Associates Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 716 (2d Cir. 1992) (quoting an earlier case).

[13]983 F. Supp. at 1167, *citing FASA Corp. v. Playmates Toys, Inc.*, 869 F. Supp. 1334, 1361–64 (N.D. Ill. 1994); *see generally supra* § 4.18[1].

[14]47 U.S.C.A. § 230(c); *Small Justice LLC v. Xcentric Ventures LLC*, 873 F.3d 313, 322-23 (1st Cir. 2017) (affirming dismissal of certain aspects of plaintiff's unfair competition based on the CDA); *Caraccioli v. Facebook, Inc.*, 700 F. App'x 588 (9th Cir. 2017) (affirming dismissal of plaintiff's claims under California's Unfair Competition Law and various tort theories "because the basis for each of these claims is Facebook's role as a 'republisher' of material posted by a third party, and the claims are, therefore, barred by the Communications Decency Act."); *Callahan v. Ancestry.com, Inc.*, Case No. 20-cv-08437-LB, 2021 WL 783524, at *5-6 (N.D. Cal. Mar. 1, 2021) (holding Ancestry.com to be an interactive computer service provider of yearbook records, in an opinion holding it entitled to CDA immunity for California right of publicity, intrusion upon seclusion, unjust enrichment and unlawful and unfair business practices claims, arising out of defendant's use of their yearbook photos and related information in its subscription database); *Roca Labs, Inc. v. Consumer Opinion Corp.*, 140 F. Supp. 2d 1311, 1319-22 (M.D. Fla. 2015) (granting summary judgment for the defendant on plaintiff's claim for allegedly violating the Florida Deceptive and Unfair Trade Practices Act (FDUTPA)); *Doe No. 1 v. Backpage.com, LLC*, 104 F. Supp. 3d 149, 162-64 (D. Mass. 2015) (dismissing plaintiff's unfair competition claim as preempted by the CDA), *aff'd on other grounds*, 817 F.3d 12, 24-25 & n.8 (1st Cir. 2016) (expressing no opinion on the district court's holding); *see generally infra* § 37.05[5][B] (analyzing CDA preemption in greater detail and citing other cases holding unfair competition claims preempted).

law."[15] The Patent Act preempts state law claims that "offer patent-like protection to intellectual property inconsistent with the federal scheme."[16] To determine whether state law torts are in conflict with federal patent law and accordingly preempted, a court must assess a defendant's allegedly tortious conduct:

> If a plaintiff bases its tort action on conduct that is protected or governed by federal patent law, then the plaintiff may not invoke the state law remedy, which must be preempted for conflict with federal patent law. Conversely, if the conduct is not so protected or governed, then the remedy is not preempted. This approach, which considers whether a state law tort, "as-applied," conflicts with federal patent law, is consistent with that employed by the Supreme Court in cases involving preemption of state unfair competition law.[17]

Patent law will not preempt state law claims that "include additional elements not found in the federal patent law cause of action and . . . [that] are not an impermissible attempt to offer patent-like protection to a subject matter addressed by federal law."[18]

In *Associated Press v. All Headline News Corp.*,[19] the court denied defendants' motion to dismiss AP's state law unfair competition claim based on passing off, in a case where the plaintiff alleged that defendants copied AP breaking news reports and reprinted its news stories on their All Headline News ("AHN") website, either as AP reports or AHN content. In allowing plaintiff's state law unfair competition claim to proceed, the court held that the plaintiff had stated a claim

---

[15] *Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1335 (Fed. Cir. 1998), *cert. denied*, 525 U.S. 1143 (1999); *see also Sears, Roebuck & Co. v. Stiffel Co.*, 376 U.S. 225, 231 (1964) (holding that state law claims for unfair competition cannot be applied to "give protection of a kind that clashes with the objectives of the federal patent laws"); *Carson Optical, Inc. v. Prym Consumer USA, Inc.*, 11 F. Supp. 3d 317, 328-35 (E.D.N.Y. 2014) (holding that plaintiffs' state law claims that defendants engaged in unfair competition by copying and reproducing plaintiff's products were preempted by the Patent Act). *Hunter Douglas* was overruled in part on other grounds.

[16] *Dow Chemical Co. v. Exxon Corp.*, 139 F.3d 1470, 1475 (Fed. Cir. 1998), *cert. denied*, 525 U.S. 1138 (1999).

[17] *Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1336 (Fed. Cir. 1998), *cert. denied*, 525 U.S. 1143 (1999).

[18] *Rodime PLC v. Seagate Tech., Inc.*, 174 F.3d 1294, 1306 (Fed. Cir. 1999), *cert. denied*, 528 U.S. 1115 (2000).

[19] *Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454 (S.D.N.Y. 2009).

by alleging that AHN passed off AP content as its own.[20]

Depending on the type of unfair competition claim asserted, it may be possible for a database owner to assert an equivalent claim under the Lanham Act.[21]

5.04[3] Patent Preemption of State Law Claims

Unlike the Copyright Act,[1] federal patent law will be deemed to preempt state law claims only in very narrow circumstances where state law presents an obstacle to the execution and accomplishment of patent laws or offers patent-like protection to intellectual property that is inconsistent with federal law.[2]

Whether a state law claim is preempted by the Patent Act is a question governed by Federal Circuit law.[3] Federal patent law preempts a state law claim that "offer[s] patent-like protection to intellectual property inconsistent with the federal scheme."[4] A claim will survive preemption if the plaintiff "plead[s] conduct in violation of [state law] that is

---

[20]608 F. Supp. 2d at 464.

[21]*See infra* § 5.08.

[Section 5.04[3]]

[1]*See supra* §§ 5.04[1], 5.04[2] (copyright preemption in database cases); *see generally supra* § 4.18[1] (analyzing copyright preemption in greater detail).

[2]*See Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1331-37 (Fed. Cir. 1998) (patent law does not provide for explicit preemption but may create conflict preemption), *cert. denied*, 525 U.S. 1143 (1999); *Dow Chemical Co. v. Exxon Corp.*, 139 F.3d 1470, 1475 (Fed. Cir. 1998) (holding a state law claim not preempted), *cert. denied*, 525 U.S. 1138 (1999); *800 Adept, Inc. v. Murex Securities, Ltd.*, 539 F.3d 1354, 1369 (Fed. Cir. 2008) ("State tort claims against a patent holder, including tortious interference claims, based on enforcing a patent in the marketplace, are 'preempted' by federal patent laws, unless the claimant can show that the patent holder acted in 'bad faith' in the publication or enforcement of its patent."); *see also Sears, Roebuck & Co. v. Stiffel Co.*, 376 U.S. 225, 231 (1964) (holding that a state law claim for unfair competition cannot be applied to "give protection of a kind that clashes with the objectives of the federal patent laws").

[3]*Ultra-Precision Mfg. Ltd. v. Ford Motor Co.*, 411 F.3d 1369, 1376 (Fed. Cir. 2005).

[4]*Dow Chemical Co. v. Exxon Corp.*, 139 F.3d 1470, 1475 (Fed. Cir. 1998); *see also Carson Optical, Inc. v. Prym Consumer USA, Inc.*, 11 F. Supp. 3d 317, 328 (E.D.N.Y. 2014) (citing *Dow Chemical* in dismissing plaintiff's unfair competition claim under New York law as preempted by the Patent Act).

separate and independent from its patent law claim."[5] To determine whether a state law tort claim is preempted by federal patent law, a court must "assess a defendant's allegedly tortious conduct. If a plaintiff bases its tort action on conduct that is protected or governed by federal patent law, then the plaintiff may not invoke the state law remedy, which must be preempted for conflict with federal patent law."[6] Accordingly, the Federal Circuit instructs courts to consider "whether a state law tort, 'as-applied,' conflicts with federal patent law. . . ."[7] State law claims are preempted if they fail to "include additional elements not found in the federal patent law cause of action," or if they are "an impermissible attempt to offer patent-like protection to subject matter addressed by federal law."[8]

Given the scope of patent preemption, it is unlikely to arise in most database disputes.

5.05 Trespass and Conversion

5.05[1] Trespass to Chattels

Common law trespass potentially provides a basis for a database owner to exclude third parties from accessing its site or service, but in California a plaintiff must show harm in the form of diminishment of server capacity, which may be difficult today given that large commercial websites typically maintain ample capacity and that entities seeking to scrape data from a site often time their access to off-peak hours. Other states may impose less exacting damage requirements, although the damage shown generally must be to the chattel itself and not merely an injury to the business. Some states, however, will not even recognize a

---

[5] *Veto Pro Pac, LLC v. Custom Leathercraft Mfg. Co.*, Civil Action No. 3:08–cv–00302 (VLB), 2009 WL 276369, at *2 (D. Conn. Feb. 5, 2009) (holding that "the third count of the complaint, unjust enrichment, is completely preempted as it simply incorporates the two counts of patent infringement by reference and asserts that these also constitute unjust enrichment on the part of the defendants").

[6] *Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1336 (Fed. Cir. 1998), *overruled in part on other grounds*, *Midwest Ind. Inc. v. Karavan Trailers, Inc.*, 175 F.3d 1356, 1360–61 (Fed. Cir. 1999) (en banc).

[7] *Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1336 (Fed. Cir. 1998), *overruled in part on other grounds*, *Midwest Ind. Inc. v. Karavan Trailers, Inc.*, 175 F.3d 1356, 1360–61 (Fed. Cir. 1999) (en banc).

[8] *Rodime PLC v. Seagate Tech., Inc.*, 174 F.3d 1294, 1306 (Fed. Cir. 1999).

trespass claim involving intangibles. Even where recognized, a claim potentially may be preempted by the Copyright Act or precluded by the Uniform Trade Secrets Act.

The Restatement of Torts 2d provides that one who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

(a) he dispossesses[1] the other of the chattel, or
(b) the chattel is impaired as to its condition, quality, or value, or
(c) the possessor is deprived of the use of the chattel for a substantial time, or
(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[2]

In the 1990s, Internet service providers successfully used common law trespass to chattels to prevent spammers from directing unsolicited electronic mail messages to their servers and subscribers.[3] In *CompuServe Inc. v. Cyber Promotions, Inc.*,[4] for example, a federal court in Ohio preliminarily enjoined a bulk commercial emailer liable for trespass to chattels, where the defendant had directed spam emails to plaintiff's subscribers. The court found that defendant's intrusions into CompuServe's computer system resulted in CompuServe's customers receiving unwanted bulk email messages, causing many of them to terminate their accounts. The court held that this harm to plaintiff's business reputa-

---

[Section 5.05[1]]

[1]"A dispossession may be committed by intentionally (a) taking a chattel from the possession of another without the other's consent, or . . . (c) barring the possessor's access to a chattel." Restatement (Second) of Torts § 221 (1965); *see also Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697-98 (D. Md. 2011) (holding that the plaintiff could proceed to trial on its trespass to chattels claim based on dispossession where the defendant, a former web developer employee, took down plaintiff's website and replaced it with an earlier version from 2007, holding that the issue of the defendant's intent presented a jury question precluding summary judgment).

[2]Restatement (Second) of Torts § 218 (1965). The "tort recovery requires not only [a] wrongful act plus causation reaching to the plaintiff, but proof of some harm for which damages can reasonably be assessed." *Doe v. Chao*, 540 U.S. 614, 621 (2004).

[3]*See infra* § 29.04.

[4]*CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997).

tion and goodwill was actionable.[5]

In *eBay, Inc. v. Bidder's Edge, Inc.*,[6] a federal court in San Jose extended this precedent to enjoin a competitor of eBay from repeatedly accessing and copying eBay's database through the use of bots (or intelligent agent software) where the court found that if injunctive relief was not granted "it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers . . . . [T]here appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value."[7]

By accessing eBay's site repeatedly without authorization—in violation of eBay policies—Judge Whyte concluded that Bidder's Edge committed a trespass, which could be enjoined to protect eBay from the lost server capacity caused by Bidder's Edge's repeated intrusions.[8] He conceded, however, that there was "some uncertainty as to the precise level of possessory interference required to constitute intermeddling."[9]

Subsequently, in *Intel Corp. v. Hamidi*,[10] the California Supreme Court held that a claim for trespass to chattels under California law may not be based on an electronic communication that neither damages the recipient's computer system nor impairs its functioning. In California, trespass requires a showing of intermeddling harmful to a materially

---

[5]*CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1023 (S.D. Ohio 1997).

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

[7]*eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071–72 (N.D. Cal. 2000).

[8]Bidder's Edge's bots accessed eBay's site approximately 100,000 per day, accounting for as much as 1.53% of the total requests received by eBay and as much as 1.10% of the total data transferred by it over the web.

[9]The case settled while an appeal was pending before the Ninth Circuit. Bidder's Edge agreed to abide by the terms of the injunction entered by the district court and paid eBay an undisclosed amount of money. *See* Troy Wolverton, "eBay, Bidder's Edge end legal dispute," c/net, Mar. 1, 2001.

[10]*Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1 Cal. Rptr. 3d 32 (2003). Hamidi involved bulk email transmissions sent to Intel by a disgruntled former employee. Unlike Bidder's Edge, it did not involve database access or copying.

valuable interest, rather than mere interference that does not amount to dispossession. Whereas eBay seemed to suggest that even the absence of actual damage could be actionable if a trespass occurred, the California Supreme Court disagreed with that broad a reading of the case, emphasizing that injunctive relief was justified in eBay based on the likely consequences of failing to enjoin future trespasses. Under California law, the court explained, intermeddling is actionable only if the "condition, quality, or value" of a chattel is impaired or "the possessor is deprived of the use of the chattel for a . . . time . . . so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession."[11] Relief for trespass to chattels is appropriate, the California Supreme Court explained, where the unauthorized access to a computer server "actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power."[12]

Following *Hamidi,* the court in *In re iPhone Application Litigation*[13] dismissed plaintiffs' trespass claims with prejudice in a data privacy putative class action suit where two sets of plaintiffs alleged that (1) the creation of location history files and app software components "consumed portions

---

[11]*Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1357, 1 Cal. Rptr. 3d 32 (2003).

[12]*Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1356, 1 Cal. Rptr. 3d 32 (2003). The court reached this conclusion following a discussion of *eBay* and *Ticketmaster Corp. v. Tickets.com, Inc.*, CV 99-7654 HLH (BQRx), 2000 WL 525390 (C.D. Cal. Mar. 27, 2000), *aff'd mem.*, Appeal No. 00-56574 (9th Cir. Jan. 2001). In *Tickets.com*, Judge Harry Hupp had distinguished *eBay, Inc.* because in the case before him he found insufficient evidence of "physical harm to the chattel . . . or some obstruction of its basic function." However, as underscored by the text of an initial tentative ruling that was subsequently withdrawn and replaced, Judge Hupp's analysis of *Ticketmaster's* trespass claim (as well as the contract claim discussed in section 5.03[2]) was heavily influenced by his concern that the data copied by Tickets.com was largely uncopyrightable, and that any protected content copied by Tickets.com without authorization amounted to a fair use intermediate copying (by analogy to reverse engineering). Judge Hupp wrote that "[t]he primary star in the copyright sky . . . is that purely factual information may not be copyrighted . . . Thus, unfair as it may seem . . . , the basic facts [Tickets.com] gathers and publishes cannot be protected from copying."

[13]*In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012).

of the cache and/or gigabytes of memory on their devices" and (2) apps had taken up valuable bandwidth and storage space on mobile devices and the defendants' conduct subsequently shortened the battery life of the device. In holding that plaintiffs had not met the standard set in *Hamidi,* Judge Lucy Koh of the Northern District of California explained that "[w]hile these allegations conceivably constitute a harm, they do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system, which is necessary to establish a cause of action for trespass."[14]

In another data privacy case also brought under California law, *In re Google Android Consumer Privacy Litigation*,[15] the court dismissed plaintiff's trespass to chattels claim because the alleged loss of CPU processing and battery capacity and Internet connectivity did not constitute a harm sufficient to establish a cause of action for trespass.

Judge Koh also dismissed plaintiff's trespass claim in *Brodsky v. Apple Inc.*,[16] where plaintiffs had alleged that Apple interfered with their possessory interests in Apple devices by requiring an "extraneous login process" through two-factor authentication (2FA) that allegedly was imposed without authorization or consent, and which allegedly "blocked 100%" use for "ongoing short periods of time when 2FA" was triggered or when their devices were not connected to the internet (or even locked them out for days when access to a trusted device to receive 2FA was lost), because plaintiffs alleged that 2FA added only "2-5 or more minutes" more than other login processes. Judge Koh ruled that "a delay of 2-5 minutes does not impair the functioning of Plaintiffs' Apple devices or Apple IDs" and, for any longer delays, plaintiffs failed to allege proximate causation.[17] The court also found that plaintiffs could not allege that their use of 2FA was unauthorized because plaintiffs had volunta-

---

[14]*In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012).

[15]*In re Google Android Consumer Privacy Litig.*, No. 11-MD-02264, 2013 WL 1283236, at *13 (N.D. Cal. Mar. 26, 2013).

[16]*Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 122-24 (N.D. Cal. 2020).

[17]*Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 124 (N.D. Cal. 2020). The court further held that a plaintiff locked out because he couldn't remember his password could not establish that Apple the cause of his being locked out. *See id.* at 125.

rily downloaded the software that installed it.[18]

Likewise, in *Mount v. PulsePoint, Inc.*,[19] a putative data privacy class action suit brought in federal court in New York under New York law over the defendant's alleged use of tracking cookies, the court dismissed plaintiff's trespass claim. Judge Naomi Reice Buchwald of the Southern District of New York wrote that "[t]o establish trespass to chattels, plaintiffs must show that PulsePoint intentionally, and without justification or consent, physically interfered with the use and enjoyment of personal property in their possession, and that they were harmed thereby."[20] Citing *Intel Corp. v. Hamidi*[21] and other cases that she characterized as applying the Restatement (Second) of Torts standard, Judge Buchwald explained that:

> Possessors of chattel, unlike possessors of land, are not protected from "harmless intermeddlings." Restatement (Second) of Torts § 218 cmt. e (1965). There must be a resulting harm to "the possessor's materially valuable interest in the physical condition, quality, or value of the chattel," or else the possessor must be "deprived of the use of the chattel for a substantial time" or have some other legally protected interest in the property affected. *Id.; see Kuprewicz*, 3 Misc. 3d at 281, 771 N.Y.S.2d at 807-08 (adopting Restatement standard). For this reason, as applied to the online context, trespass "does not encompass . . . an electronic communication that neither damages the recipient computer system nor impairs its functioning." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1347, 71 P.3d 296, 300 (2003); *see id*. at 1356, 71 P.3d at 306 ("In the decisions so far reviewed, the defendant's use of the plaintiff's computer system was held sufficient to support an action for trespass when it actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power.").[22]

In the case before her she held that plaintiffs had not al-

---

[18]*See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 123 (N.D. Cal. 2020).

[19]*Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *9-10 (S.D.N.Y. Aug. 17, 2016), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017).

[20]*Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *9 (S.D.N.Y. Aug. 17, 2016) (*citing Sch. of Visual Arts v. Kuprewicz*, 3 Misc. 3d 278, 281, 771 N.Y.S.2d 804, 807 (Sup. Ct. N.Y. Cty. 2003); *Chevron Corp. v. Donziger*, 871 F. Supp. 2d 229, 258 (S.D.N.Y. 2012)), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017).

[21]*Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1 Cal. Rptr. 3d 32 (2003).

[22]*Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *9 (S.D.N.Y. Aug. 17, 2016), *aff'd on other grounds*, 684 F. App'x 32 (2d

leged the necessary harm to sustain their trespass claim by alleging, at most, "some unspecified increase in the use of device storage or processing capacity, without alleging that this uptick was significant or caused any discernible effect on the operation of their devices."[23] Judge Buchwald also rejected the argument that deprivation of the use of Safari's third-party cookie blocker constituted sufficient harm, finding no authority for the proposition that "one feature of a particular software application" may be viewed as a chattel.[24]

In *WhatsApp Inc. v. NSO Group Technologies Ltd.*,[25] the court dismissed plaintiff's trespass claim, with leave to amend, where plaintiffs alleged that defendants impaired the value and quality of WhatsApp's servers by designing a program that concealed malicious code and made it appear

---

Cir. 2017).

[23]*Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *9 (S.D.N.Y. Aug. 17, 2016), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017). In so ruling, Judge Buchwald distinguished the Second Circuit's ruling in *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004), which is discussed later in this section, and a New York state trial court case, *Sch. of Visual Arts v. Kuprewicz*, 3 Misc. 3d 278, 771 N.Y.S.2d 804 (Sup. Ct. N.Y. Cty. 2003), as a case involving significant harm:

> In *Register.com, Inc. v. Verio, Inc.*, the Court relied in part on the district court's finding that the defendant's use of search robots "consumed a significant portion of the capacity of [plaintiff's] computer systems," 356 F.3d 393, 404-05 (2d Cir. 2004), and in *Kuprewicz*, the defendant had allegedly sent "large volumes" of unwanted e-mails which "depleted hard disk space, drained processing power, and adversely affected other system resources on [plaintiff's] computer system," 3 Misc. 3d at 281-82, 771 N.Y.S.2d at 808 (internal quotation marks omitted). Those cases, unlike this one, involved allegations or findings of activity that either had or threatened to have a significant effect on the capacity of computer systems.

Mount v. PulsePoint, Inc., 13 Civ. 6592 (NRB), 2016 WL 5080131, at *10 (S.D.N.Y. Aug. 17, 2016), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017).

[24]*Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *10 (S.D.N.Y. Aug. 17, 2016), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017). She explained:

> Many harmless electronic intrusions could potentially be recast as deprivations of a particular feature of an application meant to keep the electronic communication out. For example, the circumvention of a spam filter by junk e-mail could be characterized as depriving the user of his or her spam filter even if the junk e-mail had no effect whatever on the functionality of the user's e-mail service. We think such a holding would upset the principle that no action for trespass lies for harmless intermeddlings with chattel.

Id.

[25]*WhatsApp Inc. v. NSO Group Technologies Ltd*., 472 F. Supp. 3d 649 (N.D. Cal. 2020), *aff'd on other grounds,* __ F.4th __, 2021 WL 5174092 (9th Cir. 2021).

that WhatsApp, rather than defendants, sent the code. Chief Judge Hamilton of the Northern District of California reasoned that this argument conflated the impairment of the value and quality of WhatsApp's servers with the impairment to "the integrity, quality, and value of WhatsApp's services" and that *Hamidi* foreclosed consequential economic damages, and questioned whether the "loss of business reputation and customer goodwill" was cognizable under an action for trespass to chattels under California law.[26]

By contrast, in *Sotelo v. DirectRevenue, LLC*,[27] a federal court in Illinois held that the plaintiff stated a claim for trespass under Illinois law where it alleged that the defendant's spyware, which was either directly downloaded from the plaintiff or bundled with software obtained from a third party, "interfered with and damaged his personal property, namely his computer and his Internet connection, by over-burdening their resources and diminishing their functioning." In that case, the plaintiff had alleged that defendant's spyware "bombarded" users' computers with pop-up advertisements that obscured the web page a user was viewing and "destroy[ed] other software on a computer." Plaintiff also alleged that the spyware and resource-consuming advertisements sent to a computer by the spyware caused computers to slow down, use up the bandwidth of the user's Internet connection, incur increased Internet-use charges, deplete a computer's memory, utilize pixels and screen-space on monitors, require more energy because slowed computers must be kept on for longer, and reduce a user's productivity while increasing their frustration.[28]

---

[26]*WhatsApp Inc. v. NSO Group Technologies Ltd*., 472 F. Supp. 3d 649, 683-86 (N.D. Cal. 2020) (*citing Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1347, 1358, 1 Cal. Rptr. 3d 32 (2003); *Hiossen, Inc. v. Kim*, No. CV1601579SJOMRWX, 2016 WL 10987365, at *11 (C.D. Cal. Aug. 17, 2016) (holding that a financial injury resulting from trespass to a computer is not an actual harm under *Hamidi*); *Fields v. Wise Media, LLC*, No. C 12-05160 WHA, 2013 WL 5340490, at *4 (N.D. Cal. Sept. 24, 2013) (same)), *aff'd on other grounds,* __ F.4th __, 2021 WL 5174092 (9th Cir. 2021). *But see Microsoft Corp. v. Does 1–18,* No. 13cv139 (LMB/TCB), 2014 WL 1338677, at *10 (E.D. Va. Apr. 2, 2014); *CompuServe Inc. v. Cyber Promotions, Inc.,* 962 F. Supp. 1015, 1023 (S.D. Ohio 1997).

[27]*Sotelo v. DirectRevenue, LLC*, 384 F. Supp. 2d 1219, 1229-33 (N.D. Ill. 2005).

[28]*Sotelo v. DirectRevenue, LLC*, 384 F. Supp. 2d 1219, 1230 (N.D. Ill.

In *Craigslist Inc. v. 3Taps Inc.*,[29] a federal court in California likewise denied a defendant's motion to dismiss where plaintiff plausibly alleged that defendant's use of its website "could divert sufficient computing and communications resources to impair the website's and servers' functionality."[30] In that case, Craigslist also had alleged that one of the defendants "boasts that it mass copies tens of millions of postings from craigslist in 'real time.' "[31] The court conceded, however, that these allegations would need to be proven for the plaintiff to actually establish liability.

In *Grace v. Apple Inc.*,[32] Judge Koh, who had authored the *iPhone* decision, denied Apple's motion to dismiss plaintiffs' common law trespass claim under California law where the plaintiffs alleged injury from Apple allegedly permanently disabling FaceTime on its iOS6 and earlier operating systems which allegedly substantially harmed the functioning of their iPhones and significantly impaired the devices' condition, quality and value. Judge Koh distinguished her own earlier opinion in *In re iPhone Application Litigation*[33] as a case that merely alleged conduct that took up device memory and reduced battery life. Judge Koh also rejected the argument that plaintiffs had incurred no injury because they could have upgraded to iOS7 for free because plaintiffs alleged that iOS7 on their older iPhone 4 devices caused slowness, system crashes, erratic behavior and loss of critical features. In so ruling, Judge Koh adopted Judge Alsup's formulation that injury in the context of electronic trespass is adequately alleged where the plaintiff pleads that the purported trespass (1) caused physical damage to personal property, (2) impaired the condition, quality or value of the personal property, or (3) deprived plaintiff of the use of

---

2005).

[29]*Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 980-81 (N.D. Cal. 2013).

[30]*Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 981 (N.D. Cal. 2013).

[31]*Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 981 (N.D. Cal. 2013).

[32]*Grace v. Apple Inc.*, Case No. 17-CV-00551, 2017 WL 3232464 (N.D. Cal. July 28, 2017).

[33]*In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012).

personal property for a substantial time.[34]

Similarly, in *In re Lenovo Adware Litigation*,[35] Judge Ronald Whyte of the same court held that the plaintiffs in a putative class action suit stated a claim for trespass based on the operation of Superfish software loaded on Lenovo computers, where plaintiffs alleged that the software, which was constantly running in the background, interfered substantially with their use of their computers, by decreasing battery life by as much as 55% and slowing down internet upload and download speeds.

Northern District of California Judge DaVila likewise denied defendant's motion to dismiss in *Best Carpet Values, Inc. v. Google*,[36] which involved an alleged trespass claim to a website based on the display of advertisements that were alleged to obscure and block plaintiff's site, over objections that plaintiff had suggested no cognizable injury because Google's search app did not affect how plaintiffs' websites function or how they are displayed by other programs. *Best Carpet* is an odd opinion, given that Google's search app doesn't alter third party websites, but is perhaps best understood as a decision on a rule 12 motion where the court allowed the case to move forward at that stage in the proceedings.

Even where consent is provided, courts have recognized that "consent to enter may be limited and that a trespass claim may lie when the scope of consent is exceeded."[37] In *San Miguel v. HP Inc.*,[38] for example, Judge Davila held that plaintiffs stated a claim for trespass where they alleged that HP exceeded its authorized access to their printers when it activated a firmware update that allegedly disabled their

---

[34]*Grace v. Apple Inc.*, Case No. 17-CV-00551, 2017 WL 3232464, at *11 (N.D. Cal. July 28, 2017), *quoting Fields v. Wise Media, LLC*, No. C 12–05160 WHA, 2013 WL 5340490, at *4 (N.D. Cal. Sept. 24, 2013).

[35]*In re Lenovo Adware Litig.*, Case No. 15-md-02624-RMW, 2016 WL 6277245, at *8-9 (N.D. Cal. Oct. 27, 2016).

[36]*Best Carpet Values, Inc. v. Google LLC*, Case No. 5:20-cv-04700-EJD, 2021 WL 4355337, at *4-6 (N.D. Cal. Sept. 24, 2021)

[37]*In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 455 (N.D. Cal. 2018) (holding that plaintiffs stated a claim for trespass where they alleged that iOS updates were designed to slow their iPhones' processing speed, which impaired the condition, quality, or value of their devices, and that plaintiffs were not informed of this fact).

[38]*San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1088 (N.D. Cal. 2018).

printers and rendered their non-HP cartridges unusable.[39]

By contrast, in *Fields v. Wise Media, LLC*,[40] Judge William Alsup dismissed plaintiffs' trespass claim without leave to amend where plaintiffs had alleged that defendants interfered with their mobile phones by sending unsolicited text messages where plaintiffs could allege neither physical harm nor impairment to their phones as a result of the messages. Plaintiffs, Judge Alsup wrote, alleged "a financial injury that did not result from the physical damage or interference with their phones."[41]

Similarly, in *In re Apple & ATTM Antitrust Litigation*,[42] the court held that the loss of use of a personal iPhone for a few days, before plaintiffs received free replacements, was not a sufficient injury to establish Article III standing to maintain a claim for trespass to chattels based on harm allegedly caused by an update to the iOS operating system.[43] In so ruling, the court contrasted the "loss of commercial email servers in a large corporation for a 'substantial' or 'measurable' time . . . ," which had been found sufficient harm to support a claim in *Intel v. Hamidi*.[44] The court also held that plaintiffs failed to introduce evidence to show loss based on third party software applications which allegedly had become inaccessible, where there was no evidence that the plaintiffs paid for the apps or that they had been lost due to the iOS software upgrade, as opposed to other reasons

---

[39]In so ruling, the court relied on *In re Apple & AT & TM Antitrust Litigation*, 596 F. Supp. 2d 1288, 1307 (N.D. Cal. 2008) for the proposition that consent limited to installation of a software update did not foreclose a trespass claim. As noted in the text below, however, the court in *AT & TM* subsequently granted summary judgment for Apple on plaintiff's trespass claim. *See In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010). Ultimately, it may be easier for a plaintiff to allege a claim for computer trespass than to actually prove the elements of a claim.

[40]*Fields v. Wise Media, LLC*, No. C 12-05160 WHA, 2013 WL 5340490, at *4-5 (N.D. Cal. Sept. 24, 2013).

[41]*Fields v. Wise Media, LLC*, No. C 12-05160 WHA, 2013 WL 5340490, at *5 (N.D. Cal. Sept. 24, 2013).

[42]*In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965 (N.D. Cal. July 8, 2010).

[43]*In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965, at *6 (N.D. Cal. July 8, 2010) (entering summary judgment for defendants).

[44]*See Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1352-53, 1 Cal. Rptr. 3d 32 (2003).

suggested in plaintiffs' deposition testimony, such as user deletion or the interaction with another software application.[45]

In the alternative, the court held that even if plaintiffs could establish standing, there was no evidence of intentional interference, which is a required element of a claim for trespass to chattels.[46] The court explained that there was no evidence that Apple intended to harm plaintiffs' devices. In addition, because plaintiffs voluntarily downloaded the iOS upgrade, "[v]oluntary installation runs counter to the notion that the alleged act was a trespass . . . ."[47]

In *Register.com, Inc. v. Verio, Inc.*,[48] the Second Circuit affirmed entry of a preliminary injunction under New York law based on trespass to chattels based on evidence that the plaintiff's computer systems were valuable resources of finite capacity, unauthorized use of the systems depleted the capacity available to end-users, and unauthorized use created risks of congestion and overload that could have disrupted plaintiff's operations.[49]

The Second Circuit neither cited to *Hamidi* nor imposed as exacting a standard for injury under New York law. Rather than suggesting that a significant reduction in server capacity had to be shown or threatened, the Second Circuit affirmed the district court's reliance on *eBay* for the proposition that "any interference with an owner's use of a portion of its property causes injury to the owner."[50] The Second Circuit explained that a trespass to chattel occurs under New York law when a party intentionally damages or interferes with the use of property belonging to another, where interference may be accomplished by "dispossessing

---

[45]*In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010).

[46]*In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010).

[47]*In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010).

[48]*Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 438–39 (2d Cir. 2004).

[49]The court emphasized that "the chattels in question are Register.com's computer systems, and the alleged trespass is Verio's intentional, unauthorized consumption of the capacity of those systems to handle, process and respond to queries." *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437 n.55 (2d Cir. 2004).

[50]*Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 438 (2d Cir. 2004) (emphasis added).

another of the chattel" (which does not require a showing of actual damage) or "using or intermeddling with a chattel in the possession of another" which requires a showing of actual damage.[51] In *Register.com*, the Second Circuit accepted the district court's findings that Verio's unauthorized use of software robots posed a risk to the integrity of Register.com's systems due to potential congestion and overload problems that were shown to pose risks that were "real and potentially disruptive of its operations . . . ."[52]

In *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*,[53] a court in Ohio held that genuine issues of fact precluded summary judgment on a database owner's claim for trespass against a competitor that accessed its database to copy proprietary information ostensibly belonging to a client (with the client's permission), where its access caused the database owner's servers to crash and slow down run times, leading to customer complaints.

Snap-On was an electronic parts catalog provider to clients in the automotive and heavy equipment industries, including Mitsubishi Caterpillar Forklift. Snap-On customers such as Mitsubishi typically provided raw data, such as parts catalogs, to Snap-On, which in turn created a searchable database with links to data and images. At some time after June 2005, Mitsubishi requested a copy of its data in electronic format. Snap-On offered to sell Mitsubishi a copy with minimal enhancements or, for substantially more money, provide a copy with full enhancements (hot spots,

---

[51] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437 (2d Cir. 2004).

[52] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 438 (2d Cir. 2004). Although not discussed in the Second Circuit's opinion, the evidence of harm presented to the district court showed that as much as 2.3% of Register.com's system resources were diminished by Verio's use of bots. In addition, Verio conceded that its practices occupied some of Register.com's system capacity. Indeed, evidence showed that "Verio was aware that its robotic queries could slow the response times of the registrars' databases and even overload them" and that it contemplated using IP aliasing to make it more difficult for Register.com to identify (and presumably block) its attempts to access Register.com's servers. Register.com's position was also bolstered by Verio's contention that no limit need ever be placed on the number of companies permitted to harvest data from Register.com's computers, which Judge Jones found unreasonable. *See Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004).

[53] *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 678–80 (N.D. Ohio 2010).

links and photographs). Mitsubishi, which believed that it had already paid for the enhanced data pursuant to the terms of the license and website development agreements it entered into with Snap-On, refused. Thereafter, Mitsubishi began talks with O'Neil, a competitor of Snap-On, eventually agreeing by letter agreement dated October 2008 to provide an electronic parts catalogue and parts content management services to Mitsubishi, presumably in place of Snap-On. Mitsubishi, however, did not have an electronic copy of its data to provide O'Neil and concluded it would be too expensive to have O'Neil build its own database from Mitsubishi's paper records, as Snap-On had done. Accordingly, O'Neil suggested that it could use a scraper tool to retrieve the electronic data from Snap-On's servers.

With Mitsubishi's approval and permission, O'Neil used an automated tool that it had developed to access Snap-On's database, copy information stored on the system, and save it to O'Neil's database, where O'Neil could analyze and manipulate it. O'Neil's alleged objective was to extract raw data which it could then use on its own system. Because the scraper tool mimicked a user accessing Snap-On's password-protected website, Mitsubishi gave O'Neil approximately thirty existing logon credentials to avoid detection. O'Neil ran the scraper tool for three months beginning in February 2009. According to Snap-On, its website crashed in April and May 2009 because of "enormous spikes" in website traffic caused by O'Neil's scraping sessions. In May 2009, Snap-On began blocking O'Neil's IP addresses. After obtaining indemnification from Mitsubishi, O'Neil resumed scraping Snap-On's servers using different IP addresses and randomizing the times when it accessed Snap-On's servers (presumably to avoid detection and make it more difficult for Snap-On to block O'Neil). In July 2009, Snap-On filed suit.

In denying O'Neil's motion for summary judgment, the court held that to state a claim for trespass under Ohio law, a plaintiff must show that it has a possessory interest in a chattel and that the defendant (1) dispossessed the plaintiff of the chattel; (2) impaired the chattel's condition, quality or value; (3) deprived the plaintiff of the chattel's use for a substantial time; or (4) caused bodily harm to the plaintiff or to some person or thing from which plaintiff had a legally

protected interest.[54] The court found that Snap-On had presented evidence that O'Neil's scraper program damaged Snap-On's servers (impairing the servers' condition, quality or value or depriving Snap-On of their use for a substantial time). It also held that Snap-On's claim was not preempted by the Copyright Act. Although the parties did not dispute that Snap-On had not provided permission to O'Neil to access its servers, the court held that whether Mitsubishi was authorized to grant access was a disputed fact.

Snap-On eventually obtained a general jury verdict, although it is not clear whether the verdict was based on Snap-On's claims for trespass, breach of contract (based on its EULA), copyright infringement or violations of the Computer Fraud and Abuse Act.[55]

Snap-On provides a cautionary tale on what not to do when a contract dispute arises over ownership to content in a database. In that case, Mitsubishi had signed license and web development agreements that were favorable to Snap-On and did not clearly allow it a copy of the electronic version of its data, making it difficult for Mitsubishi to ever change database hosts without incurring substantial costs.[56] Rather than negotiating a solution or seeking a declaratory judgment of its rights back in 2005 when the dispute over ownership to its data first arose, it retained a competitor in 2008 and spent significant time and money exercising self-help that eventually resulted in a judgment for Snap-On against O'Neil in 2010, for which Mitsubishi had agreed to provide indemnification to O'Neil. A case by Mitsubishi to obtain a copy of a database comprised of its own data would have been perceived differently by a judge or jury than a suit by the database company against a competitor that repeatedly

---

[54]708 F. Supp. 2d 669, 678–80, *citing CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021–22 (S.D. Ohio 1997); *see generally infra* § 29.04[4] (analyzing *Cyber Promotions*).

[55]*See Snap-On Business Solutions Inc. v. O'Neil & Associates, Inc.*, No. 5:09–CV–1547, 2010 WL 2650875 (N.D. Ohio July 2, 2010) (awarding costs but denying Snap-On's request for an award of attorneys' fees because under Ohio law contractual attorneys' fee provisions are unenforceable as contrary to public policy because they are viewed as encouraging litigation).

[56]In the absence of an agreement, a database developer will own the rights to any software or other original creative expression, even if the underlying data is owned by the customer. *See infra* § 11.02[2]. Website development agreements and their provisions are separately analyzed in chapter 19.

screen scraped a database and undertook significant measures to avoid detection.

In *Jedson Engineering, Inc. v. Spirit Construction Services, Inc.*,[57] which was also decided under Ohio law, the court granted the plaintiff's motion for summary judgment on its claim of trespass to chattels where the defendant used a password to access a website maintained by the plaintiff for a particular construction project. In rebuffing the defendant's challenge that damages could not be shown, the court accepted the plaintiff's argument that by virtue of the defendant's trespass the plaintiff "suffered harm in terms of the diminished value of servers as a safe, secure location for project files."[58]

Judge Barrett also rejected defendant's argument that the plaintiff could not maintain a claim for trespass where it did not have "possession" of its website, which was hosted by a third party. To state a cause of action for trespass to chattels under Ohio law, the court held that it was not necessary to establish that it was the owner of the property, merely that it had a superior right to possession.[59]

The court also held that plaintiff's trespass claim was not preempted by the Copyright Act.

In *A.V. v. iParadigms, LLC*,[60] the court granted summary judgment on a plagiarism website's counterclaim for trespass against a student who falsely submitted a paper to a school where he was not enrolled. The site owner alleged that it had expended significant time and resources investigating and rectifying the student's unauthorized use of the system. The court, however, held that this evidence supported a claim for consequential damages but did not evidence impairment to the condition, quality or value of the chattel (in this case, the plagiarism website) or that the site owner incurred actual damages as a result of loss of use of the chattel, which was what was required to be shown under Virginia law.

---

[57] *Jedson Engineering, Inc. v. Spirit Const. Services, Inc.*, 720 F. Supp. 2d 904 (S.D. Ohio 2010).

[58] *Jedson Engineering, Inc. v. Spirit Const. Services, Inc.*, 720 F. Supp. 2d 904, 926 (S.D. Ohio 2010).

[59] *Jedson Engineering, Inc. v. Spirit Const. Services, Inc.*, 720 F. Supp. 2d 904, 926 (S.D. Ohio 2010).

[60] *A.V. v. iParadigms, LLC*, 544 F. Supp. 2d 473, 485 (E.D. Va. 2008), *aff'd in part and rev'd in part on other grounds*, 562 F.3d 630, 639 (4th Cir. 2009).

In *Inventory Locator Service, LLC v. Partsbase, Inc.*,[61] the court likewise dismissed the plaintiff's trespass claim based on defendant's alleged unlawful access to plaintiff's database where the plaintiff did not explicitly allege interference with its physical server, as opposed to unauthorized access to its database, and where Florida trespass law required that trespass to chattels involve movable personal property, not intangible property such as a database.[62]

Similarly, in *Universal Tube & Rollform Equipment Corp. v. YouTube, Inc.*,[63] the court granted YouTube's motion to dismiss a trespass claim based on disruptions to plaintiff's *utube.com* website caused by intended visitors to YouTube mistakenly calling up plaintiff's *utube.com* website. First, the court held that trespass to chattels must be based on interference with a plaintiff's computer system, rather than its website or domain name. Under Ohio law, the court, wrote, a "chattel" is limited to property that is "visible, tangible and moveable."[64] Second, the plaintiff's claim failed because YouTube did not make contact with the computers hosting plaintiff's website. "[T]hose making contact with Universal's website were thousands of mistaken visitors, but not YouTube itself."[65] In other words, there is no claim for secondary liability for trespass to chattels.

While a database owner may seek to deter screen scraping and establish its potential entitlement to sue for trespass by including appropriate language in its Terms of Use providing that access is unauthorized,[66] *Register.com* underscores that notice that access is prohibited may simply be provided

---

[61] *Inventory Locator Service, LLC v. Partsbase, Inc.*, No. 02-2695 MA/V, 2005 WL 2179185 (W.D. Tenn. Sept. 6, 2005) (applying Florida law).

[62] By contrast, the court held that the plaintiff had stated a claim for conversion where the plaintiff alleged that the defendant hacked into the database to obtain customer passwords, accessing the entire customer list, and making changes to the database that sabotaged plaintiff's customer relations, where Florida law recognized an action for conversion based on a wrongful taking over of intangible interests in a business.

[63] *Universal Tube & Rollform Equipment Corp. v. YouTube, Inc.*, 504 F. Supp. 2d 260 (N.D. Ohio 2007).

[64] *Universal Tube & Rollform Equipment Corp. v. YouTube, Inc.*, 504 F. Supp. 2d 260, 269 (N.D. Ohio 2007).

[65] *Universal Tube & Rollform Equipment Corp. v. YouTube, Inc.*, 504 F. Supp. 2d 260, 269 (N.D. Ohio 2007).

[66] *See infra* § 22.05[2][P] (discussing anti-trespass provisions that may be employed).

by a cease and desist letter or other means. Unauthorized access also may be communicated through the Robot Exclusion Standard discussed in *eBay*[67] or through other header information.

In *Mortensen v. Bresnan Communication, LLC*,[68] a court in Montana denied an ISP's motion to dismiss Computer Fraud and Abuse Act[69] and trespass claims where the plaintiff alleged that the ISP had modified user computer settings, even as the court dismissed plaintiff's ECPA and invasion of privacy claims based on the finding that the ISP provided notice to consumers in its Privacy Notice and Subscriber Agreement that their electronic transmissions might be monitored and would in fact be transferred to third parties, and also provided specific notice via a link on its website of its use of the NebuAd Appliance to transfer data to NebuAd (and of subscribers' right to opt out of the data transfer (via a link in that notice). The court concluded that altering privacy settings and security controls was outside the scope of the access permitted by the ISP's Privacy Notice and Subscriber Agreement to constitute trespass under Montana law. The court, however, relied on pre-*Hamidi* California law and therefore did not consider whether plaintiff had alleged impairment to its computer, as opposed to merely unauthorized access. The *Mortensen* court's ruling subsequently was vacated on other grounds, based on the district court's earlier denial of the ISP's motion to compel arbitration.[70]

Where a claim of trespass may be asserted, it generally

---

[67]The Robot Exclusion Standard is a protocol that allows sites to use "robot exclusion headers" (which are messages that may be read and detected by computers that comply with the Standard) and "robots.txt." files to define the extent to which robotic activity will be permitted on a site.

Courts have held that failing to provide notice of objection in a robots.txt file could support a defense of implied license to a claim of copyright infringement, at least for the limited purpose of allowing a search engine to cache content (although an implied license potentially could be revoked). *See Parker v. Yahoo!, Inc.*, No. 07-2757, 2008 WL 4410095, at *4 (E.D. Pa. Sept. 25, 2008); *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1115-16 (D. Nev. 2006); *see generally supra* § 4.05[7] (analyzing implied licenses under copyright law and discussing these cases).

[68]*Mortensen v. Bresnan Communication, LLC*, No. CV 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Nov. 15, 2010), *vacated on other grounds*, 722 F.3d 1151 (9th Cir. 2013).

[69]18 U.S.C.A. § 1030; *infra* § 5.06.

[70]*See Mortensen v. Bresnan Communications, LLC*, 722 F.3d 1151

will not be preempted by the Copyright Act.[71] If it is based on copying information without an extra element, however, it will be preempted.[72]

Where a trespass claim is premised on the acquisition of data, it also may be preempted by the Uniform Trade Secrets Act, depending on the applicable state law. Section 7 of the UTSA provides that the Act "displaces conflicting tort, restitutionary, and other law of this State pertaining to civil liability for misappropriation of a trade secret."[73] Section 7 has been construed to preempt trespass claims premised on the wrongful taking and use of confidential business and proprietary information, even in cases where the information at issue may not constitutes a trade secret (at least in some jurisdictions).[74]

(9th Cir. 2013).

[71] *See, e.g., Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 678–80 (N.D. Ohio 2010) (holding plaintiff's trespass claim not preempted where plaintiff alleged trespass to its physical computer servers, not merely interference with possessory rights); *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1072 (N.D. Cal. 2000) ("The right to exclude others from using physical personal property is not equivalent to any rights protected by copyright and therefore constitutes an extra element that makes trespass qualitatively different from a copyright infringement claim.").

[72] *See, e.g.*, *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 650 (E.D. Pa. 2007) (holding plaintiff's trespass claim preempted and granting summary judgment in favor of the defendants where plaintiff's claim was based on defendants making allegedly unauthorized copies of archived website screen shots and website content stored on the Wayback Machine (www.archive.org), not plaintiff's servers); *see generally supra* § 4.18[1] (analyzing copyright preemption).

[73] UTSA § 7; *infra* § 10.17 (analyzing case law on UTSA preemption). A copy of the UTSA is reprinted in the appendix to chapter 10.

[74] *See, e.g.*, *Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1080 (N.D. Cal. 2018) (dismissing plaintiff's California common law trespass claim on alternative grounds; "To the extent defendants base their trespass claims on the accessing of their systems by the anti-piracy software, they must *but have not* alleged facts showing that access *impaired* the intended functioning of defendants' systems. And to the extent that defendants base their trespass claim on the anti-piracy software's securing of and use of defendants' data, that common law claim would be preempted by CUTSA."), *citing Heller v. Cepia, LLC*, No. C 11–01146 JSW, 2012 WL 13572, at *7 (N.D. Cal., Jan. 4, 2012) (common law claims, including trespass, "premised on the wrongful taking and use of confidential business and proprietary information, regardless of whether such information constitutes trade secrets, are superseded by the CUTSA."); *see generally infra* § 10.17 (discussing conflicting lines of cases on whether a

Whether a claim is viable ultimately may turn on the extent of harm incurred to servers or tangible property (and not simply business information) and the extent of harm required under applicable state law for a potential claim to be deemed actionable, assuming applicable state law allows for a cause of action for trespass to intangibles.

In addition to common law trespass, some states have enacted specific computer trespass statutes, which are addressed in section 5.06 in conjunction with an analysis of the federal Computer Fraud and Abuse Act. The CFAA provides a federal remedy for computer trespass, where the specific elements of the statute may be satisfied.

5.05[2] Conversion

Conversion typically was not a viable claim for protecting the contents of a database because unlike a claim for trespass to chattels, which may be maintained where there is unauthorized access (plus damage), conversion usually requires a showing of dispossession or at least substantial interference.[1] Under California law, for example, conversion generally is defined as "the wrongful exercise of dominion

---

claim is preempted even if it is based on information that may not be protectable as a trade secret).

[Section 5.05[2]]

[1]*See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437–38 (2d Cir. 2004) ("Traditionally, courts have drawn a distinction between interference by dispossession, . . . which does not require a showing of actual damages, . . . and interference by unauthorized use or intermeddling, . . . which requires a showing of actual damages . . . ."; citations omitted) (New York law); *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1067 (N.D. Cal. 2000) (distinguishing trespass from conversion). *But see CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (suggesting in *dicta* that less than complete dispossession may be sufficient under Ohio law; illegal use or misuse or wrongful detention of the property would be sufficient to show conversion); Restatement (Second) of Torts §§ 217 to 220.

On similar grounds, courts have generally declined to find that software can be converted. *See, e.g.*, *Rich Media Club, LLC v. Mentchoukov*, No. 2:11–CV–1202 TS, 2012 WL 1119505, at *4 (D. Utah Apr. 3, 2012) (denying a conversion of intellectual property claim in part because the plaintiff was not "deprived of the use of any of its source code, software, or access codes); *Ho v. Taflove*, 696 F. Supp. 2d 950, 957 (N.D. Ill. 2010) (granting summary judgment for the defendant on plaintiff's claim for conversion because taking a copy did not prevent the owner "from conducting, controlling, accessing, using, or publishing" their material), *aff'd on other grounds*, 648 F.3d 489, 502 (7th Cir. 2011) (holding that plaintiff's conversion claim was preempted by the Copyright Act); *Tegg Corp. v.*

over the personal property of another."[2] Similarly, under Utah law, conversion is "an act of wilful interference with a chattel, done without lawful justification by which the person entitled thereto is deprived of its use and possession."[3] Likewise, under North Carolina law, conversion requires a showing of ownership by the plaintiff and wrongful possession or conversion by the defendant.[4] When digital information is accessed without authorization, it is usually copied exactly without dispossessing the owner of the data.

By contrast, where data is actually taken or damaged, a claim for conversion may arise. For example, in *Inventory Locator Service, LLC v. Partsbase, Inc.*,[5] the court held that the plaintiff had stated a claim for conversion where the plaintiff alleged that the defendant hacked into its database to obtain customer passwords, accessing its entire customer list, and made changes to the database that sabotaged plaintiff's customer relations, where Florida law recognized an action for conversion based on a wrongful taking-over of intangible interests in a business.

Courts are gradually becoming more amenable to conversion claims involving digital information to the extent that intangible interests have been taken (assuming such a conversion claim is not preempted). In *In re Easysaver*

Beckstrom Elec. Co., 650 F. Supp. 2d 413, 432 (W.D. Pa. 2008) ("because it is intangible property, software is generally not subject to a conversion claim.").

[2]*See, e.g.*, *CRS Recovery, Inc. v. Laxton*, 600 F.3d 1138, 1145 (9th Cir. 2010). Conversion generally requires a showing of (1) plaintiff's possessory right or interest in the property and (2) defendant's exercise of dominion over the property or interference with it "in derogation of plaintiff's rights." *Colavito v. New York Organ Donor Network, Inc.*, 8 N.Y.3d 43, 49–50, 827 N.Y.S.2d 96, 860 N.E.2d 713 (2006); *see also Fremont Indem. Co. v. Fremont General Corp.*, 148 Cal. App. 4th 97, 119, 55 Cal. Rptr. 3d 621 (2d Dist. 2007) ("The basic elements of the tort [of conversion] are (1) the plaintiff's ownership or right to possession of personal property; (2) the defendant's disposition of the property in a manner that is inconsistent with the plaintiff's property rights; and (3) resulting damages.").

[3]*Fibro Trust, Inc. v. Brahman Fin., Inc.*, 974 P.2d 288, 295-96 (Utah 1999).

[4]*See Spirax Sarco, Inc. v. SSI Engineering, Inc.*, 122 F. Supp. 3d 408, 445 (E.D.N.C. 2015) (dismissing plaintiff's conversion claim in a case based on defendants' allegedly improper access to, copying and deletion of plaintiff's electronic records and trade secrets).

[5]*Inventory Locator Service, LLC v. Partsbase, Inc.*, No. 02-2695 MA/V, 2005 WL 2179185 (W.D. Tenn. Sept. 6, 2005) (applying Florida law).

Rewards Litigation,[6] for example, a court allowed a claim to go forward where plaintiffs alleged conversion based on the alleged misappropriation of their private financial information, which was then used by defendants to make allegedly unauthorized debits from their financial accounts.

Likewise, in *Teva Pharmaceuticals USA, Inc. v. Sandhu*,[7] the court held that plaintiff could state a claim for conversion of trade secrets taken from the plaintiff's computer network by an employee, but could not state a claim against the two competitors she was working with. To state a claim for conversion of trade secrets under Pennsylvania law, the court held that a plaintiff must allege that: (1) it owns a trade secret; (2) the trade secret was communicated to the defendant within a confidential relationship; and (3) the defendant used the trade secret to the plaintiff's detriment.[8] The court emphasized that intangible intellectual property could be converted under Pennsylvania law. In holding that plaintiff stated a claim against defendant Sandu, the court explained that plaintiff alleged that Sandhu knowingly provided its trade secrets and other confidential materials to Desai and Apotex, who used the trade secrets to compete with Teva, to its detriment, which was sufficient to state a claim. By contrast, the court held that Teva could not state a claim against Desai and Apotex because neither was in a confidential relationship with Teva.

Courts also may recognize conversion claims arising out of dispossession of a domain name,[9] at least in jurisdictions

---

[6]*In re Easysaver Rewards Litig.*, 737 F. Supp. 2d 1159 (S.D. Cal. 2010).

[7]*Teva Pharmaceuticals USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 680 (E.D. Pa. 2018).

[8]*Teva Pharmaceuticals USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 680 (E.D. Pa. 2018).

[9]*See CRS Recovery, Inc. v. Laxton*, 600 F.3d 1138 (9th Cir. 2010) (reiterating that "a domain name is intangible property, subject to an action for conversion under California law[,]" in a suit by a domain name registrant who allowed the mat.net registration to lapse, which then enabled the new registrant, Li Qiang, to create an email address at mat.net that matched the email address of the administrative contact for rl.com, a different registration, which Li then transferred to his own name and sold to someone in India who in turn sold it to the defendant). *But see, e.g.*, *Xereas v. Heiss*, 933 F. Supp. 2d 1, 6-7 (D.D.C. 2013) (holding that a conversion claim could not be based on a domain name registration under D.C. law); *see generally infra* § 7.23.

that recognize domain names as intangible property.[10] A federal court in New York further ruled that a plaintiff could state a claim for conversion of social media accounts (in addition to a domain name) under New York state law.[11] Personal information, however, generally has been found not to be property that can be converted.[12]

Among other defenses to conversion, a defendant may assert abandonment, which generally requires a clear, unequivocal and decisive act demonstrating a waiver of the plaintiff's property rights.[13]

A conversion claim also may not lie when premised on breach of a contract,[14] such as a TOU agreement or a Privacy

---

[10]*See infra* § 7.23 (analyzing domain names as property).

[11]*Salonclick LLC v. SuperEgo Management LLC*, 16 Civ. 2555 (KMW), 2017 WL 239379, at *4 (S.D.N.Y. Jan. 18, 2017) (holding that plaintiff had stated a claim for conversion of a domain name and social media accounts under New York law); *see also Salonclick LLC v. SuperEgo Management LLC*, 16 Civ. 2555 (KMW), 2017 WL 1906865, at *3 (S.D.N.Y. May 8, 2017) (declining to dismiss plaintiff's conversion claim as moot, where the domain name and social media accounts had been transferred to the plaintiff, because the plaintiff still could be entitled to monetary relief, including punitive damages).

[12]*See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1030–31 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for conversion because personal information does not constitute property under California law, plaintiffs could not establish damages and some of the information allegedly "converted," such as a LinkedIn user ID number, was generated by LinkedIn, and therefore not property over which a plaintiff could claim exclusivity); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1074–75 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' conversion claim because personal information does not constitute property under California law, plaintiffs failed to establish that "the broad category of information referred to as 'personal information' is an interest capable of precise definition" and the court could not conceive how "the broad category of information referred to as 'personal information' . . . is capable of exclusive possession or control.").

[13]*See, e.g., CRS Recovery, Inc. v. Laxton*, 600 F.3d 1138, 1146 (9th Cir. 2010).

[14]*See, e.g., AD Rendon Commc'n, Inc. v. Lumina Americas, Inc.*, No. 04-CV-8832 (KMK), 2007 WL 2962591, at *4 (S.D.N.Y. Oct. 10, 2007) ("[E]ven if a plaintiff meets all of the elements of a conversion claim, the claim will still be dismissed if it is duplicative of a breach of contract claim."), *citing Wechsler v. Hunt Health Systems, Ltd.*, 330 F. Supp. 2d 383, 431 (S.D.N.Y. 2004) and *Richbell Information Services, Inc. v. Jupiter Partners, L.P.*, 309 A.D.2d 288, 765 N.Y.S.2d 575, 590 (1st Dep't 2003); *AJW Partners LLC v. Itronics Inc.*, 68 A.D.3d 567, 568, 892 N.Y.S.2d 46 (1st Dep't 2009) (holding that conversion claim was properly dismissed as

Policy.

Although unlikely to arise in a database or screen scraping case, California law also recognizes a defense where an acquirer of allegedly converted property was an innocent purchaser for value.[15]

Where a claim for conversion is based on the acquisition of data, it may be preempted by the Uniform Trade Secrets Act in states that have enacted section 7 of the UTSA. That section provides that the Act "displaces conflicting tort, restitutionary, and other law of this State pertaining to civil liability for misappropriation of a trade secret."[16] Section 7 has been construed in some, but not all, jurisdictions to preempt conversion claims premised on the wrongful taking and use of confidential business and proprietary information, regardless of whether the information constitutes a trade secret.[17]

Where a claim for conversion may be stated, it will usually not be preempted by the Copyright Act because a claim for conversion presupposes dispossession or substantial interference, which would be an extra element beyond mere

---

duplicative of the breach of contract claim because it based on same alleged violation of the parties' agreement).

[15]*See CRS Recovery, Inc. v. Laxton*, 600 F.3d 1138, 1145 (9th Cir. 2010). California law distinguishes between a purchaser whose vendor obtained title by fraud (which renders title merely voidable) and a purchaser whose vendor obtained title by theft (which is void). An innocent purchase for value without notice (actual or constructive) that his vendor has secured the goods by fraudulent purchase is not liable for conversion. Where property is stolen, it is not possible to acquire title under California law and the purchaser may be held liable for conversion. *CRS Recovery, Inc. v. Laxton*, 600 F.3d 1138, 1146 (9th Cir. 2010) (citing California state cases).

[16]UTSA § 7; *infra* § 10.17 (analyzing case law on UTSA preemption). A copy of the UTSA is reprinted in the appendix to chapter 10.

[17]*See, e.g.*, *Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1080 (N.D. Cal. 2018) (dismissing plaintiff's California common law conversion claim; "As to conversion, 'if the only property identified in the complaint is confidential or proprietary information, and the only basis for any property right is trade secrets law, then a conversion claim predicated on the theft of that property is preempted' by CUTSA."), *quoting Avago Technologies U.S. Inc. v. Nanoprecision Products, Inc.*, Case No. 16-cv-03737-JCS, 2017 WL 412524, at *7 (N.D. Cal. Jan. 31, 2017); *see generally infra* § 10.17 (discussing conflicting lines of cases on whether a claim is preempted when based on information that may not be protectable as a trade secret).

copying.[18] Some courts, however, skip over the thornier issue of dispossession where it is clear that the claim is based solely on copying and is preempted.[19]

A conversion claim asserted against an interactive computer service (or user) for the misconduct of a different person or entity also may be preempted by the CDA.[20]

In most instances, conversion will not provide protection where the contents of a database are merely copied.

5.06 Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA),[1] a criminal statute, provides a trespass-like civil remedy under federal law when a third party accesses a database, website, or other protected computer, (1) without permission or (2) exceeds

---

[18]*See, e.g., Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 971-72, 989 (N.D. Cal. 2015) (holding plaintiff's conversion claim to not be preempted where plaintiffs alleged that the defendants had preloaded their devices with apps that allowed them to access plaintiffs' electronic address books and disseminate information from these files to third parties without plaintiffs' knowledge or authorization, because, in addition to reproduction, plaintiff alleged unauthorized access, transmission, misuse and misappropriation of the data); *Internet Archive v. Shell*, 505 F. Supp. 2d 755, 763–64, (D. Colo. 2007) (holding that breach of contract and conversion claims arising out of a site owner's objection to her site being copied for inclusion in the Internet Archive's Wayback machine were not preempted). *But see Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 650 (E.D. Pa. 2007) (holding plaintiff's conversion claim preempted and granting summary judgment in favor of the defendants where plaintiff's claim was based on defendants making allegedly unauthorized copies of archived website screen shots and website content stored on the Wayback Machine (www.archive.org)); *see generally supra* § 4.18[1] (analyzing copyright preemption).

[19]*See, e.g.*, *Ho v. Taflove*, 648 F.3d 489, 502 (7th Cir. 2011) (holding that plaintiff's conversion claim was preempted by the Copyright Act); *Phantomalert, Inc. v. Google Inc.*, No. 15-CV-03986-JCS, 2016 WL 879758, at *12-14 (N.D. Cal. Mar. 8, 2016) (dismissing as preempted plaintiff's conversion claim, arising out of alleged copying of certain elements of plaintiff's program in defendants' Waze app); *see generally supra* § 4.18[1] (analyzing copyright preemption).

[20]*See* 47 U.S.C.A. § 230(c)(1); *see also, e.g.*, *Franklin v. X Gear 101, LLC*, 17 Civ. 6452 (GBD) (GWG), 2018 WL 3528731, at *19 (S.D.N.Y. July 23, 2018) (dismissing claims for unjust enrichment and conversion against Instagram and GoDaddy as barred by the CDA); *see generally infra* § 37.05 (analyzing the scope of CDA preemption).

[Section 5.06]

[1]18 U.S.C.A. § 1030; *see generally infra* § 44.08.

authorized access. The CFAA "is primarily a criminal anti-hacking statute."[2] It prohibits a number of different specific acts of misconduct involving access to protected computers (and mobile phones or other computerized devices[3]). "The statute . . . provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly."[4] As explained by the Fifth Circuit, "courts have interpreted 'access without authorization' as targeting outsiders who access victim systems, while 'exceeds authorized access' is applied to 'insiders, such as employees of a victim company. . . . [The CFAA punishes] those who have no permission to access a system and those who have some permission to access but exceed it . . . .' "[5] Resolving a significant circuit split in 2021, the U.S. Supreme Court held, in *Van Buren v. United States*,[6] that "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 limits to him."[7] According to the Supreme Court, authorized access is not exceeded within the meaning of the CFAA merely because someone authorized to access a computer uses it for unauthorized purposes, such as in violation of Terms of Service.[8] There remains an open question, however, about whether the CFAA applies when publicly available informa-

---

[2]*Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, 810 F.3d 1075, 1079 (7th Cir. 2016).

[3]The definition of *computer* pursuant to 18 U.S.C.A. § 1020(e)(1) is "exceedingly broad" and encompasses a mobile phone. *United States v. Kramer*, 631 F.3d 900, 902-03 (8th Cir. 2011); *see also United States v. Nosal*, 844 F.3d 1024, 1050 n.2 (9th Cir. 2016) (citing *Kramer* for this point in *dicta*).

[4]*Musacchio v. United States*, 136 S. Ct. 709, 713 (2016).

[5]*United States v. Thomas*, 877 F.3d 591, 596 (5th Cir. 2017) (citations omitted).

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

[7]*Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021).

[8]*See Van Buren v. United States*, 141 S. Ct. 1648, 1661 (2021). Case law pre-dating *Van Buren*, where violations were based on exceeding authorized access, are no longer good law if they were premised on policy violations, such as use violations prescribed by website Terms of Service, where access to a database was otherwise permitted but the particular use (for example, for competing business services) was proscribed by the policy.

tion is scraped—either without authorization or by exceeding authorized access. That issue is addressed later in this section.

The CFAA potentially applies when information is scraped from a database. Earlier cases imposing CFAA liability for using a scraper software program to systematically extract a company's prices[9] or other data[10] (such as email addresses or customer listings)[11] from a database or to otherwise gain unauthorized access to a website[12] are no longer good law to the extent based on use violations of website or database contracts or policies (including Terms of Use), but nevertheless represent activities that are potentially actionable under the Act if undertaken without authorization or by exceeding authorized access based on access, rather than use restrictions (*i.e.*, scraping parts of a site or service for which authorization has not been provided, as opposed to a policy violation of Terms of Service or other policies).

The CFAA may be violated by former or departing employees by, for example, continuing to access a company database after employment is terminated (constituting unauthorized access)[13] but after *Van Buren* would no longer be applicable where an employee sabotages an employer's network shortly before leaving the company (while access was still autho-

---

[9]*See, e.g., EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–83 (1st Cir. 2001). This opinion was abrogated by *Van Buren v. United States*, 141 S. Ct. 1648, 1653 n.2 (2021).

[10]*See Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) (event and ticket sales information).

[11]*See Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1057 (N.D. Cal. 2010) (entering a default judgment under the CFAA).

[12]*See, e.g., CoStar Realty Information, Inc. v. Field*, 612 F. Supp. 2d 660 (D. Md. 2009) (access to a web-based database beyond what was authorized by the site's user agreement); *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, 307 F. Supp. 2d 521 (S.D.N.Y. 2004); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[13]*See, e.g.*, *Sell It Social, LLC v. Strauss*, 15 Civ. 970 (PKC), 2018 WL 2357261, at *3-4 (S.D.N.Y. Mar. 8, 2018) (denying summary judgment where there was a dispute over when, and if, Strauss had been terminated and, in turn, whether he knowingly or intentionally accessed his employer's database without authorization, where there was at least some evidence that the defendant knew he had been fired before he accessed the database and that "Strauss retained login credentials solely because SIS neglected to remove him as an administrator on Listrak and not because Strauss continued to have permission to access the database.").

rized for performing routine work functions, but was exceeded by actions taken to disable remote access and damage the network)[14] unless the sabotage occurred in areas of the network to which access otherwise was not permitted. A CFAA claim also may lie against competitors who falsely pose as someone else to use the login credentials of someone else gain access to a protected computer.[15]

Some courts have also held that intentionally targeting email or phone calls to a company to prevent it from receiving calls, emails or voicemail messages may be actionable under the CFAA.[16]

---

[14]*See United States v. Thomas*, 877 F.3d 591, 598-99 (5th Cir. 2017) (affirming the conviction of an IT employee who had authority to stop backups or delete files but did not have authority to put in place a series of harmful acts to disable remote access to the network and cause other harm after he left the company). After *Van Buren*, employee theft of trade secrets or confidential information from a company network are only actionable as CFAA violations if they were undertaken after the employee lost access to the network or if they involved areas of a network (such as files, folders, or databases) which the employee was not authorized to access. Copying or deleting files in violation of company policy or the employee's duty of loyalty, without more, would not be actionable under the CFAA. *See, e.g.*, *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 202-04 (4th Cir. 2012) (finding no liability where an employee improperly downloaded work documents to his personal computer), *cert. dismissed*, 568 U.S. 1079 (2013); *Royal Truck & Trailer Sales & Service, Inc. v. Kraft*, 974 F.3d 756, 759-63 (6th Cir. 2020) (affirming dismissal of Royal's claims against former employees for sending confidential documents to their personal email accounts before resigning to work for a competitor, in a decision applying the narrow view consistent with Van Buren; "Section 1030(a)(2)'s aim . . . is penalizing those who breach cyber barriers without permission, rather than policing those who misuse the data they are authorized to obtain."), *cert. denied*, __ S. Ct. __, 2021 WL 2405157 (2021); *Modern Remodeling, Inc. v. Tripod Holdings, LLC*, 477 F. Supp. 3d 399, 405 (D. Md. 2020) (applying the Fourth Circuit's pre-*Van Buren* narrow view of *exceeding authorized acceess* to find, consistent with *Van Buren*, that "Drab may have copied MRI files to flash drives in contravention of MRI's policy. But as in *WEC Carolina*, there is no dispute that Drab was authorized to access those files. Following the Fourth Circuit's holding in *WEC Carolina*, then, Drab's copying of documents to a USB, even if in violation of MRI policy, does not constitute unauthorized access or exceeding unauthorized access under the CFAA.").

[15]*See, e.g.*, *Podium Corp. v. Chekkit Geolocation Services Inc.*, Case No. 2:20-cv-352-DB, 2020 WL 6940737, at *2 (D. Utah Nov. 25, 2020) (denying defendant's motion to dismiss).

[16]*See Pulte Homes, Inc. v. Laborers' Int'l Union of North America*, 648 F.3d 295 (6th Cir. 2011); *see also United States v. Carlson*, 209 F. App'x 181, 185 (3d Cir. 2006) (upholding a conviction where the defendant admit-

The CFAA, as an anti-hacking statute, prohibits access, rather than copying *per se*. In contrast to a claim for common law trespass (at least in California), which also penalizes unauthorized access, diminishment of server capacity need not specifically be shown to state a CFAA claim.[17] However, to bring a claim under the CFAA a plaintiff generally must be able to show a minimum loss of $5,000 from the defendant's conduct.[18] This dollar threshold has been an obstacle in some Internet data cases where $5,000 in actual losses could not be shown (or had not been alleged).[19] There is authority for the proposition that the $5,000 threshold

---

ted sending thousands of email messages to plaintiff).

[17]*See supra* § 5.05[1].

[18]*See infra* § 44.08 (specifically enumerating all of the alternative grounds for showing loss sufficient to maintain a civil CFAA claim and identifying potentially conflicting lines of authority).

[19]*See, e.g., Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 440 (2d Cir. 2004) (finding the plaintiff not likely to prevail on its CFAA claim arising out of the defendant exceeding authorized access to plaintiff's database); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 148-49 (3d Cir. 2015) (affirming dismissal of defendants' motions to dismiss plaintiffs' CFAA claim for failure to allege the threshold loss of $5,000 in a putative data privacy class action suit where plaintiffs could not allege any viable lost marketing opportunity for their data), *cert. denied*, 137 S. Ct. 36 (2016); *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1262-63 (9th Cir. 2019) (denying leave to amend for plaintiff to add a CFAA claim as futile, where he alleged that he was denied the profits he might have received from commodifying his personal information (which Sirius XM allegedly obtained through unlawful means), because the concept of *loss* under the CFAA is narrow and "refers *only* to losses that occurred 'because of interruption of service.' 18 U.S.C. § 1030(e)(11) . . . ;" The CFAA is an anti-hacking statute, not a misappropriation statute, and "[t]he statute's 'loss' definition—with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself."); *Cottle v. Plaid Inc*., Case No. 20-cv-03056-DMR, 2021 WL 1721177, at *15-16 (N.D. Cal. Apr. 30, 2021) (dismissing plaintiffs' claim, which alleged at least $5,000 in lost value of indemnification rights, as based on speculative allegations of loss, and rejecting arguments that the monetarty threshold could be met by allegations of loss of the right to control his own data, loss of the value of his data, or loss of the right to protection of the data); *Alan Ross Machinery Corp. v. Machinio Corp.*, No. 17-cv-3569, 2018 WL 3344364, at *4 (N.D. Ill. July 9, 2018) (dismissing Alan Ross Machinery's CFAA claim, in a case alleging that Machinio scraped sales listings of industrial machinery from Alan Ross's website and duplicated those listings on its website, where Alan Ross failed to allege damage or loss, because merely copying electronic information from a computer system is not enough to establish damage under the CFAA); *Citizens Information Associates, LLC v. Justmugshots.com*, Civil No. 1-12-CV-573-LY,

may be met by harm overall to a computer system and need not be suffered by just one computer during one particular intrusion.[20] It also may include the costs associated with responding to the unauthorized intrusion.[21] Thus, in disputes between commercial entities over scraping and database access, the $5,000 threshold should not be a problem for the target company if it retains a consultant to assess the intrusion and address security concerns, although it will bar relief when claims are made by individuals who cannot quantify sufficient harm (such as in data privacy cases) or where a plaintiff has failed to incur these costs. Thus, in disputes between commercial entities over scraping and database access, the $5,000 threshold should not be a problem for the target company if it retains a consultant to assess the intrusion and address security concerns, although it will bar relief when claims are made by individuals who cannot quantify sufficient harm (such as in data privacy cases) or where a plaintiff has failed to incur these costs. Case law addressing

---

2013 WL 12076563, at *3-4 (W.D. Tex. Feb. 26, 2013) (dismissing BustedMugshots.com's CFAA claim where the plaintiff aggregated millions of publicly available arrest records on its website, which had been scraped by a competitor, JustMugShots.com, because the plaintiff made only conclusory allegations of loss); *Bose v. Interclick, Inc.,* No. 10 Civ. 9183, 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011) (dismissing with prejudice a CFAA claim alleging general impairment to the value of plaintiff's computer in a putative behavioral advertising class action suit); *Lyons v. Coxcom, Inc.*, No. 08-CV-02047-H, 2009 WL 347285 (S.D. Cal. Feb. 6, 2009) (dismissing a CFAA claim where inadequate damage was alleged); *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326 (D. Me. 2003) (inability to quantify alleged loss to computer network); *Spec Simple, Inc. v. Designer Pages Online LLC*, 56 Misc. 3d 700, 54 N.Y.S.3d 837, 842-46 (N.Y. Cty. 2017) (dismissing a CFAA claim by the operator of a virtual library (online database) for paid subscribers in architectural, interior design, engineering, and facility management professions, brought against a competitor and the operator's former client, which had an ownership interest in the competitor, claiming that the client illicitly provided the operator's proprietary information to the competitor, where the only damages alleged were for unfair competition and therefore plaintiff could not meet the $5,000 threshold); *see generally infra* § 44.08.

[20]*See Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007); *see generally infra* § 44.08.

[21]18 U.S.C.A. § 1030(g), 1030(c)(4)(A)(i)(I), 1030(e)(11); *see, e.g., A.V. v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009) (reversing the district court's entry of summary judgment for the counterclaim defendant (A.V.) and remanding the case for further consideration, where the district court erroneously excluded from consideration the costs of investigation undertaken by iParadigms to determine how A.V. had gained access to its site); *see generally infra* § 44.08.

the $5,000 threshold—and related requirements under the statute for showing damage or loss—is analyzed more extensively in section 44.08[1]. Where the $5,000 threshold cannot be met, a claim may be asserted in some cases under equivalent state anti-trespass or computer crime laws, which are discussed briefly at the end of this section 5.06.

The CFAA potentially applies extraterritorially[22] and one court has held that a civil CFAA claim could be asserted when a U.S. company is accused of scraping data from a foreign website.[23]

Many CFAA cases involving scraping from databases, and data portability, were premised on Terms of Use or other contractual or policy violations that are no longer good law after the Supreme Court's 2021 decision in *Van Buren*. For example, in *Ticketmaster LLC v. RMG Technologies, Inc.*,[24] which was decided on motion for preliminary injunction, the court found Ticketmaster likely to prevail on the merits of its claim that the defendant violated the CFAA by accessing its website in violation of Ticketmaster's Terms of Use and, for commercial purposes, accessing its database thousands of times a day.

Similarly, in *Southwest Airlines Co. v. Farechase, Inc.*,[25] the court in the Northern District of Texas denied the

---

[22]*See, e.g.*, *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 448-49 (N.D. Cal. 2018) (relying on 18 U.S.C.A. § 1030(e)(2)(B), which defines a *protected computer* to include a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."); *Ryanair DAC v. Expedia Inc.*, Case No. C17-1789RSL, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018).

[23]*See Ryanair DAC v. Expedia Inc.*, Case No. C17-1789RSL, 2018 WL 3727599 (W.D. Wash. Aug. 6, 2018) (holding that Ryanair could maintain a CFAA suit against a U.S. website accused of scraping data from its website in Ireland, in violation of its Terms of Use and denying defendant's motion to dismiss for forum non conveniens or based on comity), *citing RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100 (2016) and *WesternGeco LLC v. ION Geophysical Corp.*, 138 S. Ct. 2129, 2136 (2018). *Ryanair* addressed extraterritoriality and the proper venue for litigation. It did not address liability, which today would be governed by *Van Buren v. United States*, 141 S. Ct. 1648 (2021).

[24]*Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

[25]*Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435 (N.D. Tex. 2004).

defendant's motion to dismiss plaintiff's CFAA claim where Southwest alleged that the defendant accessed fare and scheduling information that Southwest Airlines published on its website, *southwest.com*, where Southwest directly informed the defendant that its access was unauthorized. Regardless of whether the Terms of Use formed a binding contract, the plaintiff alleged that the defendant was directly and repeatedly warned that Southwest prohibited "any deep-link, page-scrape, robot, spider or other automatic device, program, algorithm or methodology which does the same things."[26] In a later case brought by the same plaintiff, a court likewise held that Southwest Airlines adequately stated a claim for breach of the terms and conditions of its website use agreement by alleging that the defendants used automated scraping tools to access ticket pricing information from its website, causing damage.[27]

In *eBay, Inc. v. Digital Point Solutions, Inc.*,[28] the court denied defendants' motion to dismiss eBay's CFAA claim, arising out of the defendants' cookie-stuffing scheme. Defendants were accused of using software to direct users' browsers surreptitiously to the eBay site (without their knowledge), where a cookie would be deposited on their hard drive and plaintiffs in turn would earn commissions from advertising revenue. In denying the defendants' motion, the court found that their access to eBay site was unauthorized because they exceeded the scope of eBay's user agreement.

In *Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*,[29] the court denied defendants' motion for summary judgment in a screen-scraping case where defendant O'Neil, a competitor of the plaintiff Snap-On, repeatedly accessed Snap-On's database (causing it to run slowly and on two occasions, crash) to copy data for Mitsubishi, a customer who was trying to transition from Snap-On's database hosting service to O'Neil, where the issue of whether Mitsubishi was authorized to allow O'Neil to access the database on its

---

[26]*Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004).

[27]*See Southwest Airlines Co. v. Roundpipe, LLC*, 375 F. Supp. 3d 687, 706 (N.D. Tex. 2019).

[28]*eBay Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156 (N.D. Cal. 2009).

[29]*Snap-on Business Solutions Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 676–78 (N.D. Ohio 2010).

behalf was disputed. Snap-On subsequently obtained a general jury verdict, although it is not clear whether the verdict was based on Snap-On's claims for trespass, breach of contract (based on its EULA), copyright infringement or violations of the Computer Fraud and Abuse Act.[30] The case is discussed in greater detail in section 5.05 in connection with Snap-On's trespass claim.

In *Mortensen v. Bresnan Communication, LLC*,[31] a court in Montana denied an ISP's motion to dismiss CFAA and trespass claims where the plaintiff alleged the defendant had modified user computer settings, even as the court dismissed plaintiff's ECPA and invasion of privacy claims based on the finding that the ISP provided notice to consumers in its Privacy Notice and Subscriber Agreement that their electronic transmissions might be monitored and would in fact be transferred to third parties, and also provided specific notice via a link on its website of its use of the NebuAd Appliance to transfer data to NebuAd (and of subscribers' right to opt out of the data transfer (via a link included in that notice)). The court held that the defendant had been authorized by its Privacy Notice and Subscription Agreement to access plaintiff's computer, based on plaintiff's use of the service after having received notice that his use was subject to terms, but that authorized access had been allegedly exceeded by altering or tampering plaintiff's computer settings, which was not disclosed in plaintiff's Privacy Notice or Subscription Agreement.[32] The *Mortensen* court's ruling subsequently was vacated on other grounds, based on the district court's earlier denial of the ISP's motion to

---

[30]*See Snap-On Business Solutions Inc. v. O'Neil & Associates, Inc.*, No. 5:09–CV–1547, 2010 WL 2650875 (N.D. Ohio July 2, 2010) (awarding costs but denying Snap-On's request for an award of attorneys' fees because under Ohio law contractual attorneys' fee provisions are unenforceable as contrary to public policy because they are viewed as encouraging litigation).

[31]*Mortensen v. Bresnan Communication, LLC*, No. CV 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Nov. 15, 2010), *vacated on other grounds*, 722 F.3d 1151 (9th Cir. 2013).

[32]The court gave only cursory consideration to whether the plaintiff could show $5,000 in damages, assuming that the mere allegation of damage by a putative class that had not yet been certified would be sufficient. This aspect of the court's holding is inconsistent with the weight of authority. *See infra* §§ 26.15 (privacy class action suits), 44.08 (analyzing the Computer Fraud and Abuse Act in greater detail).

compel arbitration.[33]

After *Van Buren*, none of these holdings remain good law to the extent they stand for the proposition that violating contractual use restrictions (where access otherwise is permitted to a database) may constitute *exceeding authorized access* under the CFAA, although CFAA claims may be actionable where access to a network or to particular files, folders, or databases, is not permitted at all.[34] Regardless of the viability of a CFAA claim, database owners may be able to sue for breach of contract or any of the other causes of action discussed in this chapter, to the extent applicable.

Even before *Van Buren*, merely accessing a publicly accessible webpage was held not to constitute a CFAA violation.[35]

Where a claim is otherwise potentially actionable, a journalist, researcher, or other person may claim a First Amendment right to scrape data from private websites (using bots and fictitious user profiles) and publish the results of their research, as a defense to a criminal CFAA prosecution.[36]

In *Fidlar Technologies v. LPS Real Estate Data Solutions,*

---

[33]*See Mortensen v. Bresnan Communications, LLC*, 722 F.3d 1151, 1157-61 (9th Cir. 2013).

[34]*See, e.g., United States v. Lowson*, Crim. No. 10-114 (KSH), 2010 WL 9552416, at *5 (D.N.J. Oct. 12, 2010) (denying defendants' motion to dismiss where they allegedly "implement[ed] 'hacks' and us[ed] 'backdoors' to enable automated programs to purchase tickets" from online vendors).

In *Van Buren*, the Supreme Court declined to address whether access restrictions must be based on "technological (or 'code-based') limitations" to be actionable, or whether they also could be "contained in contracts or policies." *Van Buren v. United States*, 141 S. Ct. 1648, 1659 n.8 (2021).

[35]*See, e.g., Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 646–49 (E.D. Pa. 2007) (granting summary judgment for the defendants in a case where plaintiffs sued the law firm that previously had represented an opposing party in a trademark infringement suit, alleging that defendants obtained archived copies of its website without authorization from the Wayback Machine, www.Archive.org, where the copies were only accessible because of a computer malfunction that caused the Archive.org site to ignore the Robots.txt files on plaintiff's site that would otherwise have resulted in the archived pages being made publicly inaccessible; "No evidence has been presented showing that the Harding firm exceeded authorized access. The facts do not show that the Harding firm did anything other than use the Wayback Machine in the manner it was intended to be used.").

[36]*See Sandvig v. Sessions*, 315 F. Supp. 3d 1, 15-30 (D.D.C. 2018) (denying in part the government's motion to dismiss; holding that

Inc.,[37] the Seventh Circuit affirmed the lower court's entry of summary judgment, holding that a data analytics company's use of a web-harvester to obtain county land records in bulk was not actionable under the CFAA. In the words of Judge Joel Martin Flaum, writing on behalf of himself and Judges Daniel A. Manion and Ilana Rovner, Fidlar, by the lawsuit "attempt[ed] to convert its failure to prohibit LPS's action by contract into an allegation of criminal conduct."[38]

In that case, the appellate panel affirmed the lower court holding that no reasonable jury could find that LPS acted

---

researchers planning to engage in audit testing of internet real estate, hiring, and other websites through the use of bots and fictitious profiles, for research purposes, plausibly alleged a First Amendment interest in doing so, plausibly alleged that they have standing to sue, and plausibly alleged that the CFAA's access provision violates the Free Speech and Free Press Clauses of the First Amendment as applied to them). In *Sandvig*, the court opined that:

> Scraping or otherwise recording data from a site that is accessible to the public is merely a particular use of information that plaintiffs are entitled to see. The same goes for speaking about, or publishing documents using, publicly available data on the targeted websites. The use of bots or sock puppets is a more context-specific activity, but it is not covered in this case. Employing a bot to crawl a website or apply for jobs may run afoul of a website's ToS, but it does not constitute an access violation when the human who creates the bot is otherwise allowed to read and interact with that site.

Id. at 26-27. In a subsequent opinion, the court held that plaintiffs had Article III standing to raise their First Amendment concerns, but that bypassing a permission requirement in a Terms of Service agreement was not actionable as exceeding authorized access and, with respect to unauthorized access, "[n]one of their research plans . . . involve[d] bypassing authenticating 'permission requirements,' and thus none of them when executed w[ould] constitute violations of the CFAA as interpreted herein." *Sandvig v. Barr*, 451 F. Supp. 3d 73, 84-92 (D.D.C. 2020), *appeal dismissed*, No. 20-5153, 2021 WL 2525027 (D.C. Cir. June 10, 2021). In this later opinion, Judge Bates held that "a user should be deemed to have 'accesse[d] a computer without authorization,' 18 U.S.C. § 1030(a)(2), only when the user bypasses an authenticating permission requirement, or an 'authentication gate,' such as a password restriction that requires a user to demonstrate 'that the user is the person who has access rights to the information accessed . . . .' " 451 F. Supp. 3d at 89, *citing* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1664 (2003) ("[t]he key point is not that some code was circumvented but rather that the computer owner conditioned access on authentication of the user and the access was outside the authentication . . .").

[37] *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075 (7th Cir. 2016).

[38] *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075, 1084 (7th Cir. 2016).

with intent to defraud[39] where the plaintiff alleged that the defendant had undertaken a fraudulent scheme to avoid paying printing fees by accessing plaintiff's records through its own web harvester. In so ruling, the appellate panel emphasized that LPS had authority to "access the county records as a general matter" but the question presented was "whether the *way* in which it did so violated the statute."[40]

The appellate panel found no basis to support plaintiff's alleged scheme where LPS used its web-harvester even in those counties that did not charge a print fee, suggesting its goal was to accelerate data acquisition, not avoid fees. In addition, LPS continued to pay for unlimited subscriptions in all 82 counties, even though it was not logging any time by using its web-harvester. If LPS wanted to defraud the counties, the court reasoned, it could have selected a limited subscription for less money. Further, LPS did not conceal its use of the web-harvester, which was inconsistent with an intent to defraud. In addition, the evidence showed that Fidlar was aware of two other companies that used their own tools to access county records, which supported LPS's assertion that its intent was speed and efficiency, not to avoid fees. Moreover, an internal Fidlar email stated that "Fidlar *could* make screen-scraping or web-harvesting illegal with a 'simple disclaimer that states the information can't be

---

[39]18 U.S.C.A. § 1030(a)(4) punishes anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ." *Intent to defraud* is not defined in the statute, but according to the Seventh Circuit means "that the defendant acted willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for himself or causing loss to another." *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075, 1079 (7th Cir. 2016) (quoting earlier cases). Because direct evidence of intent is often unavailable, intent to defraud may be established by circumstantial evidence "and by inferences drawn from examining the scheme itself, which demonstrate that the scheme was reasonably calculated to deceive persons of ordinary prudence and comprehension." *Id.* (quoting an earlier case; affirming the lower court's entry of summary judgment in a civil case finding no intent to deceive where the defendant used a web-harvester to copy county land records in bulk, and was not expressly prohibited from doing so by contract).

The legislative history of section 1030(a)(4) reflects a Congressional intent to "reach cases of computer theft. . . . The intent to defraud element is meant to distinguish computer theft from mere trespass." *Id., citing* S. Rep. No. 99-432, at 9, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486-87.

[40]*Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075, 1080 (7th Cir. 2016) (emphasis in original).

scraped from the image' " but didn't do so, suggesting that Fidlar itself "did not believe that web-harvesting was impermissible."[41] Finally, and significantly, the court noted that the agreements between LPS and the counties did not prohibit LPS from using a web-harvester or require LPS to access records exclusively through the plaintiff's program.

The Seventh Circuit also affirmed the lower court judgment that LPS did not violate section 1030(a)(5)(A), which punishes anyone who knowingly causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer.[42] Fidlar's claim, by contrast, the court wrote, was "trespassory in nature. LPS accessed the middle tier servers without following Fidlar's 'rules' (i.e., logging its activity or using the Laredo client)."[43] *Damage,* however, is defined as "any impairment to the integrity or availability of data, a program, a system or information . . . ,"[44] which the court explained contemplated destructive behavior, such as using a virus or destroying data, not merely circumventing the plaintiff's method for tracking user activity without altering any data or disrupting Fidlar's

---

[41]*Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075, 1082 (7th Cir. 2016).

[42]The phrase *without authorization* modifies different actions in section 1030(a)(5)(A) than section 1030(a)(5)(C) (an intent to cause damage without authorization, in section 1030(a)(5)(A), and accessing a protected computer without authorization, in section 1030(a)(5)(C)). *See In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 451-53 (N.D. Cal. 2018) (holding that iPhone owners alleging that Apple degraded their phones' battery performance through iOS updates stated a claim under section 1030(a)(5)(A) because even though the iPhone owners consented to install the iOS updates, they did not consent to throttling of their phones' processor speeds); *San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1085-86 (N.D. Cal. 2018) (denying HP's motion to dismiss plaintiffs' section 1030(a)(5)(A) claim where plaintiffs alleged they authorized a software update, but not damage to their printers, explaining that a claim under section 1030(a)(5)(C) would require a showing that the defendant exceeded authorized access to a protected computer); *see also In re Apple Inc. Device Performance Litig.*, 386 F. Supp. 3d 1155, 1181-82 (N.D. Cal. 2019) (granting reconsideration and reaffirming the court's prior rulings dismissing plaintiffs' section 1030(a)(5)(C) claim but not their claim under section 1030(a)(5)(A)). Scraping claims would more typically be brought under section 1030(a)(5)(C).

[43]*Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075, 1085 (7th Cir. 2016).

[44]18 U.S.C.A. § 1030(e)(8).

system in any way.[45]

Finally, the court affirmed summary judgment for LPS on Fidlar's claim under the Illinois Computer Crime Prevention Law,[46] which requires a showing that a defendant knew or had reason to know that its insertion or attempt to insert a program into a computer would cause loss. Because LPS believed that "it was entitled to download records without incurring a fee, it follows that LPS did not know or have reason to know that it was causing a loss."[47]

As noted earlier, prior to June 2021, there was a pronounced circuit split over whether a CFAA violation for exceeding authorized access could be premised on a contractual or policy violation. While a number of courts had held that accessing a website for purposes prohibited by website Terms of Use or other use restrictions constituted exceeding authorized access under the CFAA in civil cases where a conscious violation had been shown, in the Second, Fourth, Sixth and Ninth Circuits a CFAA claim for *exceeding authorized access* could not be based on a defendant's violating a contract or policy that imposes use, rather than access restrictions.[48] For example, a contract provision that allowed access for particular uses—such as personal but not com-

---

[45]*Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075, 1084 (7th Cir. 2016).

[46]720 ILCS § 5/17-51(a)(4)(C).

[47]*Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.,* 810 F.3d 1075, 1085-86 (7th Cir. 2016).

[48]*See United States v. Valle*, 807 F.3d 508, 524-28 (2d Cir. 2015); *Royal Truck & Trailer Sales & Service, Inc. v. Kraft*, 974 F.3d 756, 759-63 (6th Cir. 2020), *cert. denied*, __ S. Ct. __, 2021 WL 2405157 (2021); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*); *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 568 U.S. 1079 (2013); *see also Teva Pharmaceuticals USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 669-71 (E.D. Pa. 2018) (agreeing with the Fourth and Ninth Circuit's narrow approach and holding that plaintiff failed to state a claim against an employee who was permitted to access plaintiff's computer in the course of her employment to access information in its database, including the information allegedly shared with the other defendants); *Hedgeye Risk Management, LLC v. Heldman*, 271 F. Supp. 3d 181, 193–95 (D.D.C. 2017) (collecting cases and agreeing with the Second, Fourth and Ninth Circuits in holding that the prohibition on *exceeding authorized access* only applies to unauthorized access to information, not to unauthorized use of properly accessed material); *Tank Connection, LLC v. Haight*, 161 F. Supp. 3d 957, 969-70 (D. Kan. 2016) (granting summary judgment for a former employee who was accused of improperly accessing files on his employer's network, where the employer mistakenly had not

mercial use—was not actionable in the Second, Fourth, Sixth or Ninth Circuits,[49] but potentially could be asserted in the First, Fifth, Seventh, Eighth and Eleventh Circuits.[50] As

---

blocked access to the files as intended; "Case law makes clear that the relevant question is whether he was authorized to access the area or the information, not whether he did so with an improper purpose in mind."); *Cloudpath Networks, Inc. v. SecureW2 B.V.*, 157 F. Supp. 3d 961, 983 (D. Colo. 2016) (agreeing "with Second, Fourth, and Ninth Circuits' shared conclusion: 'exceeds authorized access' in the CFAA does not impose criminal liability on individuals who are authorized to access company data but do so for disloyal purposes; it applies only to individuals who are allowed to access a company computer and use that access to obtain data they are not allowed to see for any purpose."); *see generally infra* § 44.08 (analyzing these cases in greater detail).

[49]*See United States v. Valle*, 807 F.3d 508, 524-28 (2d Cir. 2015); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*); *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 568 U.S. 1079 (2013); *Royal Truck & Trailer Sales & Service, Inc. v. Kraft*, 974 F.3d 756, 759-63 (6th Cir. 2020), *cert. denied*, __ S. Ct. __, 2021 WL 2405157 (2021); *see generally infra* § 44.08[1] (analyzing *Nosal* case law and the current circuit split).

In *Oracle America, Inc. v. Service Key, LLC*, No. C 12-00790, 2012 WL 6019580 (N.D. Cal. Dec. 3, 2012), for example, the court dismissed Oracle's CFAA claim against a third party that accessed its website to provide software support services to third parties. Oracle had argued that the defendant was not allowed to access its website and therefore acted without authorization within the meaning of the statute, but the court ruled that Oracle's claim was barred by *Nosal* because Oracle's complaint alleged that the defendant was authorized to access its website, but not for the ostensibly improper purpose of using its authorized access to provide support services to third parties. *See id.* at *5.

[50]*See, e.g.*, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583–84 (1st Cir. 2001) (holding that an employee likely exceeded his authorized access when he used that access to disclose information in violation of a confidentiality agreement into which the employee voluntarily entered); *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) (holding that an employee of Citigroup exceeded her authorized access when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud, writing that a violation occurs "at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime . . . ."); *International Airport Centers, LLC v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006) (reversing dismissal of a claim against an employee who accessed plaintiff's network and caused transmission of a program that caused damage to a protected computer where the court held that an employee who had decided to quit and violate his employment agreement by destroying data breached his duty of loyalty to his employer and therefore terminated the agency relationship, making his conduct unauthorized (or exceeding authorized access)); *United States v.*

explained by the Second Circuit, a person exceeds authorized access under the narrow view applied in that circuit (and ultimately by the U.S. Supreme Court) "only when he obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access."[51]

In *Van Buren v. United States*,[52] the U.S. Supreme Court adopted the narrow view, holding that "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 limits to him."[53]

In that case, Van Buren, a police officer, was convicted of a felony violation of the CFAA for "exceeding authorized access," where he accessed the Georgia Crime Information Center database (which he was otherwise authorized to use for his official duties as a police officer) to run a license plate

---

Teague, 646 F.3d 1119, 1121–22 (8th Cir. 2011) (upholding the conviction under section 1030(a)(2) and 1030(c)(2)(A) of an employee of a government contractor who used his privileged access to a government database to obtain President Obama's private student loan records); *United States v. Van Buren*, 940 F.3d 1192, 1207-08 (11th Cir. 2019) (affirming the CFAA conviction of Van Buren, a police officer, for "exceeding authorized access," where he accessed the Georgia Crime Information Center database (which he was otherwise authorized to use for his official duties as a police officer) to run a license plate check for a third party for a $6,000 payment, to determine if the tag he was searching for belonged to a police officer), *rev'd*, 141 S. Ct. 1648 (2021); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that a Social Security Administration employee exceeded authorized access by obtaining information about former girlfriends and potential paramours to send flowers to their houses, where the Administration told the defendant that he was not authorized to obtain personal information for nonbusiness reasons).

These opinions were abrogated by *Van Buren v. United States*, 141 S. Ct. 1648, 1653 n.2 (2021). Although the U.S. Supreme Court only cited some of these opinions, and omitted reference to *United States v. Teague*, 646 F.3d 1119, 1121-22 (8th Cir. 2011), *Teague* is no longer good law in light of *Van Buren*.

[51] *United States v. Valle*, 807 F.3d 508, 511 (2d Cir. 2015).

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

[53] *Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021). The Court wrote that *exceeds authorized access* – which is defined in 18 U.S.C.A. § 1030(e)(6) to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"—"is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access." *Id.* at 1655.

check for a third party for a $6,000 payment, to determine if the tag he was searching for belonged to a police officer. The Supreme Court reversed his conviction, ruling that in the context of computers *exceeding authorized access* is consistent "with the act of entering a part of the system to which a computer user lacks access privileges."[54]

Justice Barrett, writing for the 6-3 majority, characterized section 1030(a)(2) as establishing "a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system."[55] In so ruling, Justice Barrett endorsed Van Buren's explanation of section 1030(a)(2) as an anti-hacking statute that protects against both external and internal hacking:

> The "without authorization" clause . . . protects computers themselves by targeting so-called outside hackers—those who "acces[s] a computer without any permission at all." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (C.A.9 2009); *see also Pulte Homes, Inc. v. Laborers' Int'l Union of North Am.*, 648 F.3d 295, 304 (C.A.6 2011). . . . [T]he "exceeds authorized access" clause . . . provide[s] complementary protection for certain information within computers. It does so . . . by targeting so-called inside hackers—those who access a computer with permission, but then " 'exceed' the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend." *United States v. Valle*, 807 F.3d 508, 524 (C.A.2 2015).[56]

While the Court relied on statutory construction—principally the definition of *exceeding authorized access* under the CFAA, and how that term fits into the overall scheme of the statute—Justice Barrett also observed that the broader view of *exceeding authorized access* "would attach criminal penalties to a breathtaking amount of commonplace computer activity."[57] She explained:

> If the "exceeds authorized access" clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals. Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So on the

---

[54] *Van Buren v. United States*, 141 S. Ct. 1648, 1657-58 (2021).

[55] *Van Buren v. United States*, 141 S. Ct. 1648, 1658-59 (2021).

[56] *Van Buren v. United States*, 141 S. Ct. 1648, 1658 (2021).

[57] *Van Buren v. United States*, 141 S. Ct. 1648, 1661 (2021). This policy perspective, Justice Barrett characterized as "extra icing on a cake already frosted." *Id, quoting Yates v. United States*, 574 U.S. 528, 557 (2015) (Kagan, J., dissenting).

> Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA. Or consider the Internet. Many websites, services, and databases—which provide "information" from "protected computer[s]," § 1030(a)(2)(C)—authorize a user's access only upon his agreement to follow specified terms of service. If the "exceeds authorized access" clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers. And indeed, numerous amici explain why the Government's reading of subsection (a)(2) would do just that—criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook.[58]

Under the approach adopted by the Supreme Court and previously applied in the Second, Fourth, Sixth, Ninth Circuits, an individual could not exceed authorized access, within the meaning of the CFAA, by accessing a computer, "with an improper purpose . . . to obtain or alter information that he is otherwise authorized to access . . . ."[59] By contrast, accessing files on a network beyond those which an employee was authorized to view meets the statute's definition of "exceeds authorized access."[60]

Applying this narrower view of the scope of *exceeding authorized access* in an earlier case, a Ninth Circuit panel held that Terms of Use prohibitions on the use of bots, scrapers, and other automated means to access a site may not form the basis for claims under either California's Computer Data Access and Fraud Act[61] or Nevada's Computer Crimes Law,[62] because "taking data using a *method* prohibited by the applicable terms of use, when the taking itself generally is

---

[58]*Van Buren v. United States*, 141 S. Ct. 1648, 1661 (2021). The Court also observed that the Government's approach (reflecting the law in the First, Fifth, Seventh, Eighth and Eleventh Circuits) "would inject arbitrariness into the assessment of criminal liability." *Id.* at 1662.

[59]*United States v. Valle*, 807 F.3d 508, 511 (2d Cir. 2015); *see also, e.g., Satmodo, LLC v. Whenever Communications, LLC*, Case No. 17-cv-0192-AJB NLS, at *5 (S.D. Cal. Apr. 14, 2017) (dismissing plaintiff's CFAA claim in a click fraud case, where the plaintiff alleged improper access by (a) violating the terms and conditions of the search engine's advertising contracts, and (b) accessing plaintiff's website after the plaintiff blocked various IP addresses).

[60]*Space Systems/Loral, LLC v. Orbital ATK, Inc.*, 306 F. Supp. 3d 845, 852 (E.D. Va. 2018).

[61]Cal. Penal Code § 502(c).

[62]Nev. Rev. Stat. §§ 205.511(1), 205.4765.

permitted, does not violate . . .” either state statute.[63]

Even under the narrow view of the scope of *exceeding authorized access* under the CFAA adopted by the Supreme Court, it may be possible for a database owner to use the CFAA to prevent screen scraping by simply revoking access. For example, while the Ninth Circuit ruled *en banc* in *United States v. Nosal*,[64] that the phrase *exceeds authorized access* does not extend to violations of use restrictions, such as those found in employment policies and website Terms of Use agreements, four years later the Ninth Circuit affirmed the defendant's conviction on the same facts for accessing the same computer system *without authorization.*[65] In that case, David Nosal, an employee at Korn/Ferry, left to start his own competing executive search firm. Although Korn/Ferry explicitly revoked Nosal's computer access credentials, Nosal continued accessing Korn/Ferry computers and information by using the password of his former executive assistant, who remained authorized to access Korn/Ferry's computers.[66] Although in its first, *en banc* opinion, in 2012, the Ninth Circuit held that Nosal could not be prosecuted for exceeding authorized access, the appellate court subsequently upheld his conviction for accessing Korn/Ferry computers without authorization, in its later opinion in 2016. The court explained

---

[63]*Oracle USA, Inc. v. Rimini Street, Inc.*, 879 F.3d 948, 961-62 (9th Cir. 2018) (reversing judgment for Oracle on claims under California and Nevada law), *rev'd on other grounds,* 139 S. Ct. 873 (2019) (reversing an award of costs to Oracle, as the prevailing party, which had included costs beyond the six categories enumerated in 28 U.S.C.A. § 1920) (emphasis in original). In *Rimini Street*, the defendant used an automated tool, in violation of Terms of Use restrictions, to download in bulk customer support files that were available for individual download. The court explained, “Oracle obviously disapproved of the method—automated downloading—by which Rimini took Oracle's proprietary information. But the key to the state statutes is whether Rimini was authorized in the first instance to take and use the information that it downloaded. . . . Because it indisputably had such authorization, at least at the time it took the data in the first instance, Rimini did not violate the state statutes.” *Id.* at 962.

[64]*United States v. Nosal,* 676 F.3d 854, 862-63 (9th Cir. 2012) (*en banc*). This opinion was written by Chief Judge Alex Kozinski. Judge Barry G. Silverman filed a dissenting opinion, in which Judge Tallman concurred.

[65]*United States v. Nosal,* 844. F.3d 1024 (9th Cir. 2016). The opinion in *Nosal* was written by Judge Margaret M. McKeown, on behalf of herself and Chief Judge Sidney R. Thomas. Judge Stephen Reinhardt filed a dissent.

[66]*United States v. Nosal,* 844 F.3d 1024, 1034-41 (9th Cir. 2016).

that *without authorization* is "an unambiguous, nontechnical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[67] As applied to Nosal, the court explained that the definition "has a simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party."[68] Hence, the court held that Nosal didn't simply exceed authorized access; "the 'without authorization' prohibition of the CFAA extends to a former employee whose computer access credentials have been rescinded but who, disregarding the revocation, accesses the computer by other means."[69]

Likewise, in *Facebook, Inc. v. Power Ventures, Inc.*,[70] the Ninth Circuit held that a company that accessed Facebook's servers to scrape data with the permission of their joint customers, but in violation of Facebook's Terms of Use agreement, nonetheless could be held civilly liable for accessing Facebook's computers *without authorization,* where Facebook sent Power Ventures a cease and desist letter advising Power Ventures that it was not permitted to do so. In that case, Power Ventures, a rival social network that allowed its users to aggregate and manage their social network accounts from different services including Facebook, ran a promotion offering its users the opportunity to win $100 by signing up 100 new Power.com friends. If a Power.com user clicked on an icon that included the words "Yes, I do!" then Power

---

[67]*United States v. Nosal,* 844 F.3d 1024, 1028 (9th Cir. 2016).

[68]*United States v. Nosal,* 844 F.3d 1024, 1028 (9th Cir. 2016).

[69]*United States v. Nosal,* 844 F.3d 1024, 1029-30 (9th Cir. 2016). The Fourth Circuit had earlier concluded, consistent with this view, that "an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer. Thus, he accesses a computer 'without authorization' when he gains admission to a computer without approval." *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012), *cert. dismissed*, 568 U.S. 1079 (2013); *see also Pulte Homes, Inc. v. Laborers' Int'l Union of North America,* 648 F.3d 295, 303-04 (6th Cir. 2011) (" 'authorization' is '[t]he conferment of legality; . . . sanction.' Commonly understood, then, a defendant who accesses a computer 'without authorization' does so without sanction or permission . . . [and] *has no rights, limited or otherwise,* to access the computer in question.' "; emphasis in original, quoting 1 Oxford English Dictionary 798 (2d ed. 1989) and *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)).

[70]*Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058 (9th Cir. 2016).

Ventures would create an event, photo or status update on the user's Facebook page. The court conceded that this process "arguably gave Power permission to use Facebook's computers to disseminate messages."[71] However, because Facebook sent Power Ventures a cease and desist letter informing Power Ventures that it was violating Facebook's Terms of Use and demanding that Power Ventures "stop soliciting Facebook users' information, using Facebook content, or otherwise interacting with Facebook through automated scripts[,]" the Ninth Circuit held that Facebook had expressly rescinded permission to access its site.[72]

Although Facebook's cease and desist letter referenced a Terms of Use violation, and the Ninth Circuit conceded that under *Nosal,* exceeding authorized access as stated in a Terms of Use agreement wouldn't be actionable, at least in the Ninth and Fourth Circuits, the panel explained in a footnote that the reference to Facebook's Terms of Use was not dispositive because the cease and desist letter also "warned Power that it may have violated federal and state law and plainly put Power on notice that it was no longer authorized to access Facebook's computers."[73]

The court also emphasized that after it received the cease and desist letter, Power Ventures knew it no longer had authorization, but continued to access Facebook's computers anyway. After sending the letter, Facebook blocked access to Facebook's website from Power Ventures' IP addresses,

---

[71] *Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1067 (9th Cir. 2016). The court elaborated that:

> Power reasonably could have thought that consent from Facebook users to share the promotion was permission for Power to access Facebook's computers. In clicking the "Yes, I do!" button, Power users took action akin to allowing a friend to use a computer or to log on to an e-mail account. Because Power had at least arguable permission to access Facebook's computers, it did not initially access Facebook's computers "without authorization" within the meaning of the CFAA.

Id.

[72] *Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1067 (9th Cir. 2016).

[73] *Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1067 n.3 (9th Cir. 2016). The court also observed that "[b]ecause, initially, Power users gave Power permission to use Facebook's computers to disseminate messages, we need not decide whether websites such as Facebook are presumptively open to all comers, unless and until permission is revoked expressly." *Id.* n.2, *citing* Orin S. Kerr, *Norms of Computer Trespass,* 116 Colum. L. Rev. 1143, 1163 (2016) (asserting that "websites are the cyber-equivalent of an open public square in the physical world").

which "further demonstrated that Facebook has rescinded permission for Power to access Facebook's computers."[74] Power Ventures internal emails showed that it was aware that Facebook was blocking its IP addresses but continued to access the Facebook site. In addition, the panel found significant the fact that "a Power executive sent an e-mail agreeing that Power engaged in four 'prohibited activities' [using a person's Facebook account without Facebook's authorization, using automated scripts to collect information from the site, incorporating Facebook's site in another database, and using Facebook's site for commercial purposes]; acknowledging that Power may have 'intentionally and without authorization interfered with [Facebook's] possessory interest in the computer system,' while arguing that the 'unauthorized use' did not cause damage to Facebook; and noting additional federal and state statutes that Power 'may also be accused of violating,' " . . .[75]

The appellate panel explained that the consent that Power Ventures received from Facebook users to access their accounts "was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission."[76] Accordingly, the court held that effective on the date it received Facebook's cease and desist

---

[74]*Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1068 (9th Cir. 2016). The court cautioned, however, that "[s]imply bypassing an IP address, without more, would not constitute unauthorized use." *Id.* n.5. The court explained that:

> Because a blocked user does not receive notice that he has been blocked, he may never realize that the block was imposed and that authorization was revoked. Or, even if he does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user's roommate or co-worker.

Id.

[75]*Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1067-68 (9th Cir. 2016).

[76]*Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1068 (9th Cir. 2016). The court offered the following analogy:

> Suppose that a person wants to borrow a friend's jewelry that is held in a safe deposit box at a bank. The friend gives permission for the person to access the safe deposit box and lends him a key. Upon receiving the key, though, the person decides to visit the bank while carrying a shotgun. The bank ejects the person from its premises and bans his reentry. The gun-toting jewelry borrower could not then reenter the bank, claiming that access to the safe deposit box gave him authority to stride about the bank's property while armed. In other words, to access the safe deposit box, the person needs permission both from his friend (who controls access to the safe) and from the bank (which controls access to its premises). Similarly, for Power to continue its campaign

letter, Power Ventures' access to Facebook's computers was *without authorization* within the meaning of the CFAA.[77] On similar grounds, the appellate panel also affirmed the entry of judgment in favor of Facebook on its claim under the California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502).[78]

---

using Facebook's computers, it needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers). Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter.

Id.

[77]A similar outcome was reached in *Tech Systems, Inc. v. Pyles,* 630 F. App'x 184, 186 (4th Cir. 2015) (affirming that once she was no longer employed, "Pyles accessed her corporate email account and company-issued Blackberry without authorization."); *see also United States v. Shahulhameed,* 629 F. App'x 685 (6th Cir. 2005) (affirming the defendant's conviction where, a few hours after he was fired, a cyberattack was launched from his Toyota-assigned laptop; rejecting the defendant's argument that his access to his former employer's network at the time was authorized because his account was not disabled until 8 hours later because "Toyota's failure to disable his account does not mean his access was authorized . . . .").

[78]Cal. Penal Code § 502; *Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1069 (9th Cir. 2016) (affirming liability under section 502 where the defendant continued to access Facebook's servers after having received a cease and desist letter instructing it to stop doing so); *see also, e.g.*, *San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1086-88 (N.D. Cal. 2018) (holding that plaintiffs stated plausible claims under subsection 502(c)(1) based on the defendant providing a firmware update that allegedly caused an error message because plaintiffs used non-HP printer cartridges, and under sections 502(c)(4) and 502(c)(5) based upon the alleged alteration and disruption caused by the firmware update to a "computer network," which is defined in section 501(b)(2) to include "printers connected by telecommunication facilities."). A claim under section 502 is similar to a claim under the federal Computer Fraud & Abuse Act, 18 U.S.C.A. § 1030, except that "the California statute does not require *unauthorized* access. It merely requires *knowing* access." *United States v. Christensen,* 828 F.3d 763, 789 (9th Cir. 2016) (emphasis in original). *Access*, according to the Ninth Circuit, "includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly." *Id.*

Although at the margin there may be a difference in a given case between no authorization (or exceeding authorization) and knowing access, section 502 and CFAA claims often are decided in tandem. *See, e.g., In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010) (granting summary judgment for defendant Apple on plaintiffs' CFAA, section 502 and common law trespass to chattels claims where the plaintiffs alleged injury arising from their installation of iOS 1.1.1., which allegedly caused damage to their iPhones

On remand, the district court in *Power Ventures* awarded $79,640.50 in damages under the Computer Fraud and Abuse Act for losses incurred on or after the date that Facebook revoked consent by sending the cease and desist letter and entered a permanent injunction pursuant to the Computer Fraud and Abuse Act and Cal. Penal Code § 502.[79]

---

and made certain third party apps inaccessible, because plaintiffs voluntarily installed the software upgrade and "[v]oluntary installation runs counter to the notion that the alleged act was a trespass and to [the] CFAA's requirement that the alleged act was 'without authorization' as well as the CPC's requirement that the act was 'without permission.' " (citing 18 U.S.C.A. § 1030(a)(5)(A)(1) (which requires a showing that a defendant "intentionally caus[ed] damages without authorization) and Cal. Penal Code §§ 502(b)(10) (which requires the knowing introduction of "computer instructions that are designed to . . . damage."), 502(c)(4) (which requires a showing that a defendant knowingly accessed and without permission added, altered, damaged, deleted, or destroyed any data, computer software, or computer programs which resided or existed internally or externally to a computer, computer system, or computer network)).

[79]*See Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765 (N.D. Cal. 2017), *aff'd mem.*, 749 F. App'x 557, 558 (9th Cir. 2019). The court entered the following permanent injunction under the CFAA:

> 1. Defendants, their agents, officers, contractors, directors, shareholders, employees, subsidiary companies or entities, affiliated or related companies and entities, assignees, and successors-in-interest, and those in active concert or participation with them, are permanently enjoined from:
>
> A. Accessing or using, or directing, aiding, facilitating, causing, or conspiring with others to use or access the Facebook website or servers for any commercial purpose, without Facebook's prior permission, including by way of example and not limitation for the purpose of sending or assisting others in sending, or procuring the sending, of unsolicited commercial electronic text messages via the Facebook website or service.
>
> B. Using any data, including without limitation Facebook-user data and data regarding Facebook's website or computer networks, obtained as a result of the unlawful conduct for which Defendants' have been found liable.
>
> C. Developing, using, selling, offering for sale, or distributing, or directing, aiding, or conspiring with others to develop, sell, offer for sale, or distribute, any software that allows the user to engage in the conduct found to be unlawful.
>
> 2. Defendants, their agents, officers, contractors, directors, shareholders, employees, subsidiary companies or entities, affiliated or related companies and entities, assignees, and successors-in-interest, and those in active concert or participation with them shall destroy any software, script(s) or code designed to access or interact with the Facebook website, Facebook users, or the Facebook service. They shall also destroy Facebook data and/or information obtained from Facebook or Facebook's users, or anything derived from such data and/or information.
>
> 3. Within three calendar days of entry of this permanent injunction and order, Defendants shall affirm that they already have notified, or shall notify, their current and former officers, agents, servants, employees, successors, and as-

In entering injunctive relief, the district court noted that "[n]umerous courts have found that unauthorized access of computers and the acquisition of data in violation of the CFAA constitute irreparable harm."[80] The court subsequently awarded Facebook $145,028.40 in attorneys' fees under section 502.[81]

---

signs, and any persons acting in concert or participation with them of this permanent injunction.

4. Within seven calendar days of entry of this injunction and order, Defendants shall certify in writing, under penalty of perjury, that they have complied with the provision of this order, and state how notification of this permanent injunction in accordance with paragraph 3 above was accomplished, including the identities of all email accounts (if any) used for notification purposes.

5. The Court shall continue to retain jurisdiction over the parties for the purpose of enforcing this injunction and order.

252 F. Supp. 3d at 785-86, *aff'd mem.*, 749 F. App'x 557, 558 (9th Cir. 2019).

[80]*See Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 782-86 (N.D. Cal. 2017) (citing *TracFone Wireless, Inc. v. Adams*, 98 F. Supp. 3d 1243, 1252-53, 1255-56 (S.D. Fla. 2015) (permanently enjoining the defendant pursuant to the CFAA and Lanham Act where, among other things, "TracFone would be irreparably harmed because Adams' actions, if allowed to persist, will continue to cause TracFone to suffer harm by impairing the integrity of TracFone's proprietary computer system and wireless telecommunications network."), *aff'd mem.*, 749 F. App'x 557 (9th Cir. 2019); *Reliable Property Services, LLC v. Capital Growth Partners, LLC,* 1 F. Supp. 3d 961, 965 (D. Minn. 2014) (preliminarily enjoining a copyright owner that accessed the plaintiff—snow removal service's computer system, disabled a program, and stole confidential customer information, finding a "substantial threat of irreparable harm" based on the public dissemination of information after the defendant "unlawfully took volumes of detailed data" in violation of the CFAA); *Enargy Power Co. v. Wang,* Civil Action No. 13–11348–DJC, 2013 WL 6234625, at *10 (D. Mass. Dec. 3, 2013) (preliminarily enjoining the defendant subject to a $10,000 bond because, among other things, "prevent[ing] Enargy from enjoying the uninterrupted use of its property. . . constitutes irreparable harm. Furthermore, Plaintiffs' inability to make use of the PH Project files has hampered Enargy. . . .") (internal citations omitted); *see also Tagged, Inc. v. Does 1 through 10,* No. C 09–01713 WHA, 2010 WL 370331, at *12 (N.D. Cal. Jan. 25. 2010) (permanently enjoining the defendant in part because of the likelihood that the defendant might violate the CFAA and Cal. Penal Code § 502 again in the future).

[81]*See Facebook, Inc. v. Power Ventures, Inc.,* Case No. 08-CV-05780, 2017 WL 3394754, at *6-8 (N.D. Cal. Aug. 8, 2017). Judge Koh wrote in dicta that section 502 allows only prevailing plaintiffs to recover fees. *See id.* at *6. For purposes of section 502, a party is a "prevailing party" if they have a "net monetary recovery" within the meaning of Cal. Code Civ. Proc. § 1032(a)(4). 2017 WL 3394754, at *6.

In *WhatsApp Inc. v. NSO Group Technologies Ltd.*,[82] the court held that Facebook stated a claim against NSO Group for exceeding authorized access where defendants created WhatsApp accounts that they caused to be used to send malicious code to third party devices. In denying defendants' motion to dismiss WhatsApp's CFAA claim, Chief Judge Phyllis Hamilton of the Northern District of California emphasized that defendant's conduct was alleged to have not only violated WhatsApp's terms of service but involved creating a program that went beyond restrictions imposed on access to technical call settings by evading WhatsApp's security features and manipulating technical call settings. In distinguishing *Nosal*, the court emphasized that "[a]voiding technical restrictions goes beyond any contractual limitations imposed by the terms of service."[83] Likewise, the court distinguished *LinkedIn* because, unlike in that case, "[t]he information defendants are alleged to have protected from access by generally applicable access permissions."[84]

In *Ticketmaster LLC v. Prestige Entertainment West, Inc.*,[85] the court, following *Power Ventures*, denied defendants' motion to dismiss plaintiff's claims under the CFAA and California Computer Data Access and Fraud Act, where Ticketmaster had sent the defendant a letter demanding that it stop accessing the Ticketmaster site using bots to make automated purchases of thousands of tickets to the popular show *Hamilton*, but the defendant continued to do so anyway.

In *Teva Pharmaceuticals USA, Inc. v. Sandhu*,[86] the court held that plaintiff failed to state a claim against Barinder Sandhu, an employee who was permitted to access plaintiff's computer in the course of her employment to access informa-

---

[82]*WhatsApp Inc. v. NSO Group Technologies Ltd.*, 472 F. Supp. 3d 649, 680-82 (N.D. Cal. 2020), *aff'd on other grounds*, __ F.4th __, 2021 WL 5174092 (9th Cir. 2021).

[83]*WhatsApp Inc. v. NSO Group Technologies Ltd.*, 472 F. Supp. 3d 649, 682 (N.D. Cal. 2020), *aff'd on other grounds*, __ F.4th __, 2021 WL 5174092 (9th Cir. 2021).

[84]*WhatsApp Inc. v. NSO Group Technologies Ltd.*, 472 F. Supp. 3d 649, 682 (N.D. Cal. 2020), *aff'd on other grounds*, __ F.4th __, 2021 WL 5174092 (9th Cir. 2021).

[85]*Ticketmaster LLC v. Prestige Entertainment West, Inc.*, 315 F. Supp. 3d 1147, 1167-76 (C.D. Cal. 2018).

[86]*Teva Pharmaceuticals USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 669-71 (E.D. Pa. 2018).

tion in its database, including the information she allegedly shared with the other defendants, but that Teva could state a CFAA claim against those other defendants, who, as outsiders, were "akin to hackers," and who plausibly could be held liable for acting in concert with Sandhu, for directing, encouraging, or inducing her to access the Teva computer system, which they were unauthorized to do.

In *Craigslist Inc. v. 3Taps Inc.*,[87] an earlier opinion, a district court in the Ninth Circuit also found revocation of consent under the CFAA based on a cease and desist letter. In that case, the court ruled that Craigslist had stated a claim for a CFAA violation against a company that scraped classified ads from its website. The court considered that by making classified advertisements publicly available on its website, Craigslist had authorized the world to access Craigslist.org.[88] The court found that Craigslist revoked its authorization, however, when it sent the defendant a cease and desist letter banning it from using the site. Judge Breyer ruled that a website owner has the power to revoke authorization to access its site and therefore the defendant acted without authorization when it continued to scrape data from Craigslist's website after the time it had received Craigslist's cease and desist letter.

By contrast, in *hiQ Labs, Inc. v. LinkedIn Corp.*,[89] Judge Edward Chen of the same district held that hiQ raised serious questions about LinkedIn's entitlement to relief under the CFAA (and California Penal Code § 502), in granting a preliminary injunction prohibiting LinkedIn from blocking hiQ's access, copying or use of public profiles on LinkedIn's website (information which LinkedIn members had designated as public) or blocking or putting in place technical or legal mechanisms to block hiQ's access to these public

---

[87] *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013).

[88] *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013), *citing Pulte Homes, Inc. v. Laborer's Int'l Union of North America*, 648 F.3d 295, 304 (6th Cir. 2011) (stating that the public presumptively was authorized to access an "unprotected website"); *see also CollegeSource, Inc. v. AcademyOne, Inc.*, Civil Action No. 10-3542, 2012 WL 5269213, at *14 (E.D. Pa. Oct. 25, 2012) (holding that documents available to the general public on the plaintiff's website could not be accessed without authorization).

[89] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985 (9th Cir. 2019).

profiles, in an opinion that was upheld on appeal.[90] In that case, LinkedIn had sent a cease and desist letter demanding that hiQ, a company that provided information to businesses about their workforces based on statistical analyses of public profiles on LinkedIn, stop using bots to automatically scrape its site. hiQ instead filed suit for injunctive relief, claiming that its data analytics business was "wholly dependent" on LinkedIn's public data, which it alleged that it had been accessing for more than five years prior to receiving the cease and desist letter. In expressing serious questions about LinkedIn's entitlement to relief under the CFAA, the court held that the CFAA "was not intended to police traffic to publicly available websites on the Internet . . . ."[91] The Ninth Circuit affirmed, emphasizing that it was merely confirming that hiQ established serious questions going to the merits, having established that the balance of hardships tipped decidedly in its favor, and thus it was not erroneous for Judge Chen to have entered a preliminary injunction. The appellate court did not decide the merits of the dispute definitively.

In ruling that the CFAA was not intended to restrict access to publicly available websites, the district court had looked beyond the language of the statute and even its legislative history to focus on "the Act's theoretical underpinning . . . as a statute addressing the problem of computer 'trespass' . . ."[92] and its "historical context . . . ."[93] Relying on a law review article by Professor Orin Kerr, Judge Chen explained that "because the Web is generally perceived as 'inherently open,' in that it 'allows anyone in the world to publish information that can be accessed by anyone else without requiring authentication,' . . . 'authorization,' in the context of the CFAA, should be tied to an authentication system, such as password protection . . . ."[94]

Although hiQ did not have to use a password to access

---

[90] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019).

[91] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985 (9th Cir. 2019).

[92] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1111 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985 (9th Cir. 2019).

[93] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985 (9th Cir. 2019).

[94] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1112 (N.D. Cal. 2017) (citing Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161-62 (2016)), *aff'd on other grounds*, 938 F.3d 985 (9th

public information from LinkedIn's site, LinkedIn required use of CAPTCHA — a program designed to allow humans, but not bots, to access its site—and had challenged both hiQ's access *and* its automatic scraping of data. LinkedIn alleged that hiQ used bots to automatically access its site and circumvent CAPTCHA restrictions. Judge Chen, however, construed *authorization* to refer to "the *identity* of the person accessing the computer or website, not *how* access occurs."[95] Citing Professor Kerr, Judge Chen concluded that by circumventing CAPTCHA, hiQ did not access LinkedIn *without authorization* within the meaning of the CFAA because:

> Unlike a password gate, a CAPTCHA does not limit access to certain individuals; it is instead intended "as a way to slow . . . a user's access rather than as a way to deny authorization to access." . . . Other measures taken by website owners to block or limit access to bots may be thought of in the same way. A user does not "access" a computer "without authorization" by using bots, even in the face of technical countermeasures, when the data it accesses is otherwise open to the public. Thus, under Professor Kerr's analysis, hiQ's circumvention of LinkedIn's measures to prevent use of bots and implementation of IP address blocks does not violate the CFAA because hiQ accessed only publicly viewable data not protected by an authentication gateway.[96]

In holding that he had serious reservations about whether LinkedIn's revocation of permission to access public portions of its site rendered hiQ's access "without authorization,"

Cir. 2019). Judge Chen also noted that the U.S. Supreme Court, in *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017), analogized the Internet in general, and social networking sites in particular, to the "modern public square . . . ." *Id.* at 1737. In that case, Judge Chen explained, the Court struck down a North Carolina law making it a felony for a registered sex offender to access social media websites like Facebook and Twitter, writing that "at present, social media sites are for many people 'the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge.' " 273 F. Supp. 3d at 1112, *quoting Packingham v. North Carolina*, 137 S. Ct. 1730, 1737 (2017). This First Amendment restriction on a state's ability to restrict access to websites, needless to say, would not transfer directly to private disputes where there is no government action.

[95] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017) (emphasis in original), *aff'd*, 938 F.3d 985 (9th Cir. 2019).

[96] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017) (footnote omitted) (citing Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1170 (2016)), *aff'd*, 938 F.3d 985, 1002 (9th Cir. 2019).

Judge Chen distinguished *Power Ventures* and *Nosal* as cases that did not involve public data.[97]

For the same reasons, Judge Chen concluded that hiQ raised serious questions about whether LinkedIn had a claim under "the California analog to the CFAA," California Penal Code § 502, which prohibits *knowing access*.[98]

On appeal, the Ninth Circuit affirmed the lower court's order on narrow grounds, subject to the deferential standard that a preliminary injunction should be affirmed absent an abuse of discretion. The appellate court found no abuse of discretion in concluding that hiQ would have suffered irreparable injury absent injunctive relief (because it allegedly would have gone out of business) or that the balance of hardships tipped sharply in hiQ's favor (on similar grounds). Based on these findings, the appellate court determined that, consistent with the traditional balancing test for granting equitable relief, hiQ was only required to show "serious questions going to the merits," which it had done.

Considering LinkedIn's potential CFAA claim as potentially supporting a "legitimate business purpose" defense to HiQ's claim for tortious interference with contract, the appellate panel drew a sharp distinction between "information presumptively accessible to the general public and information for which authorization is generally required" consistent with the panel's analysis that the CFAA is "best understood as an anti-intrusion statute and not as a 'misappropriation statute' . . . ."[99]

The panel opined that the CFAA's prohibition on access

---

[97] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017), *aff'd*, 938 F.3d 985, 1002 (9th Cir. 2019).

[98] *hiQ Labs, Inc. v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1115 n.13 (N.D. Cal. 2017) (distinguishing *Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29, 34, 65 Cal. Rptr. 3d 701 (2007) (noting that "[s]ection 502 defines 'access' in terms redolent of 'hacking' or breaking into a computer")), *aff'd on other grounds*, 938 F.3d 985, 999 n.10 (9th Cir. 2019) (resting on the CFAA and declining to address section 502). Judge Chen wrote that "[t]hough the statute also includes a provision that prohibits 'knowingly access[ing] and without permission tak[ing], cop[ying], or mak[ing] use of any data from a computer, computer system, or computer network,' Cal. Pen. Code § 502(c)(2), the Court similarly concludes there are serious questions about whether these provisions criminalize viewing public portions of a website." 273 F. Supp. 3d at 1115 n.13.

[99] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1000-04 (9th Cir. 2019).

"without authorization" did not apply to "the selective denial of access" where "free access without authorization" otherwise is permitted, which the court deemed more akin to a ban.[100] While this interpretation is debatable, the court concluded, in the alternative, that the term "without authorization" was ambiguous, and that the legislative history confirmed its construction because the CFAA is best understood as an anti-intrusion statute, not one that prohibits misappropriation.[101] Because the conduct at issue was not akin to "breaking and entering," the panel held that hiQ raised serious questions about the statute's applicability. The appellate panel further justified drawing a "distinction between information presumptively accessible to the general public and information for which authorization is generally required . . ." by reference to Ninth Circuit case law construing the Stored Communications Act.[102] In so ruling, the court distinguished cases where "authorization or access permission, such as password authentication, . . ." was required.[103] Thus, presumably, a different outcome could be warranted,

---

[100]*See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 999-1000 (9th Cir. 2019).

[101]*See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1000 (9th Cir. 2019).

[102]*hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1002-03 (9th Cir. 2019), *citing Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875, 879 n.8 (9th Cir. 2002) (explaining that, in enacting the Stored Communications Act, "Congress wanted to protect electronic communications that are configured to be private" and are " 'not intended to be available to the public.' "). The *hiQ* court elaborated that:

> Our understanding that the CFAA is premised on a distinction between information presumptively accessible to the general public and information for which authorization is generally required is consistent with our interpretation of a provision of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq*., nearly identical to the CFAA provision at issue. *Compare* 18 U.S.C. § 2701(a) ("[W]hoever—(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . unauthorized access to a wire or electronic communication . . . shall be punished . . . .") *with* 18 U.S.C. § 1030(a)(2)(C) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished . . . .").

hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1002-03 (9th Cir. 2019).

[103]*hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019). The panel elaborated that

> the CFAA contemplates the existence of three kinds of computer information: (1) information for which access is open to the general public and permission is not required, (2) information for which authorization is required and has been

even under the Ninth Circuit's analysis, for content only accessible with a password or posted on a social network such as LinkedIn and set to private or accessible only to a limited group of users, as opposed to publicly available[104]—although the decision is not entirely clear whether this would be true even for third party information made accessible only to members who log on to a service with a password. The majority elaborated that the data at issue in *hiQ* was "not owned by LinkedIn" or "demarcated by LinkedIn as private" using "an authorization system."[105] Ownership, however, should not be determinative, since many companies license content owned by third parties. Presumably, information either owned by a site or service (or potentially licensed to it) *or* accessible only by password or other authorization or access permission system could be protected by the CFAA under *hiQ*.

A narrow reading of *hiQ* would require the use of passwords or other uniformly applied restrictions for the use of content to be deemed "without authorization" under the CFAA.

A broader reading, however, would limit the use of contractual restrictions (even where passwords or similar restrictions are in place) where the information at issue is not owned or at least licensed to the site or service seeking to restrict access, similar to the U.S. Supreme Court's limitation in *Van Buren* (and the Ninth Circuit's earlier limitation in *United States v. Nosal*)[106] on use restrictions under the "exceeding authorized access" prong of the CFAA.

The Ninth Circuit panel in *hiQ* emphasized that database

---

given, and (3) information for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed). Public LinkedIn profiles, available to anyone with an Internet connection, fall into the first category. With regard to such information, the "breaking and entering" analogue invoked so frequently during congressional consideration has no application, and the concept of "without authorization" is inapt.

Id. at 1001-02.

[104] *See generally infra* § 50.06[4][C][i] (analyzing the impact of privacy settings in cases involving subpoenas and court orders under the Electronic Communications Privacy Act, which includes as Title II the Stored Communications Act).

[105] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003-04 (9th Cir. 2019).

[106] *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (*en banc*).

owners or other "entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply . . . ," citing cases recognizing common law trespass to chattels, copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy (which are addressed elsewhere in this chapter), as potentially applicable.[107] Although not mentioned by the court, circumventing CAPTCHA also potentially could constitute a violation of the anti-circumvention provisions of the Digital Millennium Copyright Act,[108] whether or not actionable under the CFAA.

The panel acknowledged that website and database owners may act to "thwart denial-of-service attacks and block[] abusive users, identity thieves, and other ill-intentioned actors[,]" noting that the district court had made clear that the injunction did "not preclude LinkedIn from continuing to engage in 'technological self-help' against bad actors—for example, by employing 'anti-bot measures to prevent, *e.g.*, harmful intrusions or attacks on its server.' "[109] In balancing public interest considerations, however, the court found more concerning the prospect of giving companies "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— [which] risks the possible cre-

---

[107]*hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1004 (9th Cir. 2019). These claims are addressed in other sections of this chapter.

[108]*See, e.g.*, *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1055–57 (N.D. Cal. 2010) (entering a default judgment for violations of sections 1201(a)(2) and 1201(b)(1) and awarding $470,000 in statutory damages under the DMCA where the defendant marketed products that circumvented plaintiff's CAPTCHA software and telephone verification security measures); *Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096, 1111–12 (C.D. Cal. 2007) (holding that Ticketmaster was likely to prevail on its DMCA claims under section 1201(a)(2) (trafficking in a device that circumvents technological measures that control access to a protected work) and 1201(b)(1) (for trafficking in a device that circumvents technological measures that protect the rights of a copyright owner in a work) relating to circumvention of CAPTCHA); *see generally infra* § 5.07[1] (addressing the anti-circumvention provisions of the DMCA).

[109]*hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1005 (9th Cir. 2019) (footnote omitted). hiQ subsequently asserted antitrust claims against LinkedIn, which were dismissed for failing to define a product market and adequately allege anticompetitive conduct. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 485 F. Supp. 3d 1137 (N.D. Cal. 2020).

ation of information monopolies that would disserve the public interest."[110]

The Ninth Circuit panel emphasized the very preliminary nature of rulings involving motions for preliminary injunctions, where a court is not called upon to actually decide a point of law as much as to determine whether a lower court abused its discretion (and in this case in finding merely serious questions going to the merits). Judge Wallace, concurring in the decision, stated more pointedly that he was

> concern[ed] that "in some cases, parties appeal orders granting or denying motions for preliminary injunctions in order to ascertain the views of the appellate court on the merits of the litigation." *Sports Form, Inc. v. United Press Int'l, Inc.*, 686 F.2d 750, 753 (9th Cir. 1982); *see also California v. Azar*, 911 F.3d 558, 583–84 (9th Cir. 2018). . . . I emphasize that appealing from a preliminary injunction to obtain an appellate court's view of the merits often leads to "unnecessary delay to the parties and inefficient use of judicial resources." *Sports Form*, 686 F.2d at 753. These appeals generally provide "little guidance" because "of the limited scope of our review of the law" and "because the fully developed factual record may be materially different from that initially before the district court." *Id.*[111]

In applying *hiQ Labs, Inc. v. LinkedIn Corp.*, it is important to keep in mind the procedural posture of the case. First, suit was filed by hiQ, seeking to enjoin enforcement, rather than by LinkedIn, to obtain affirmative relief under the CFAA. Second, because hiQ sought a preliminary injunction, the court merely found substantial questions going to the merits of the applicability of the CFAA—not ultimate liability. Third, for injunctive relief to obtain, the court was required to find irreparable harm, which in *hiQ* arose in part because hiQ's business depended on access to public profiles on LinkedIn and previously had had access for many years, which may not be true in every scraping case. Fourth, in weighing the balance of hardships, which a court must do in evaluating requests for injunctive relief, the court considered that hiQ alleged that it had had access to public profiles on LinkedIn for five years, which was also a unique factor that might not be present in every case.

It also remains to be seen whether other courts will accept

---

[110] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1005 (9th Cir. 2019).

[111] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1005-06 (9th Cir. 2019) (Wallace, J. concurring).

the Ninth Circuit's narrow construction of what constitutes *without authorization*, given that the distinction drawn between publicly available and restricted access data, in construing the seemingly unambiguous term "without authorization," is not apparent from the face of the statute.

Ultimately, these cases suggest that a database owner may restrict access by contract, employment agreement, Terms of Use, cease and desist letter, or otherwise, but it may not maintain a CFAA claim for exceeding authorized access based on a use restriction, and if the information is made publicly accessible a CFAA claim for accessing a protected computer "without authorization" also may be unavailable. *Power Ventures* and *Craigslist*, by contrast, underscore that a simple letter may be the most effective way to establish that access is not authorized (or, if it was authorized, that authorization has been revoked)—at least for data not made generally available to the public.

To maximize enforceability under the CFAA, companies that seek to protect data and databases should, where possible, impose access restrictions on the data itself (files, folders or databases), rather than use restrictions. Data also should not be made freely available to the public if a business wants to restrict access through the CFAA throughout the United States.

In addition to corporate exposure, personal liability also may be imposed under the CFAA. In *Facebook, Inc. v. Power Ventures, Inc.*,[112] the Ninth Circuit affirmed the entry of judgment for Facebook against Power Ventures and its CEO. The appellate court ruled that corporate officers or directors, in general, are personally liable for all torts which they authorize or direct or in which they participate, notwithstanding that they acted as agents for the corporation and not on their own behalf.[113] The appellate court noted, however, that personal liability typically is only imposed on corporate officers where the officer has been the *guiding spirit* behind the wrongful conduct.[114]

A claim under the CFAA must be brought within two years

---

[112]*Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069-70 (9th Cir. 2016).

[113]*Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016), *citing Committee for Idaho's High Desert, Inc. v. Yost*, 92 F.3d 814, 823 (9th Cir. 1996).

[114]*Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir.

of the date of the act complained of or the date of discovery of the damage.[115]

In limited circumstances a claim brought against a platform, intermediary or other interactive computer service for the misconduct of users could be preempted by the Communications Decency Act.[116]

The CFAA is analyzed in greater detail (along with conflicting lines of cases construing the statute) in section 44.08. CFAA claims in data privacy class action suits are analyzed in section 26.15.

In addition to CFAA claims, a number of states have enacted computer crime statutes that may provide additional remedies. Some of these statutes have been construed to be consistent with the CFAA,[117] while others are more akin to

---

2016), *citing Davis v. Metro Products, Inc.*, 885 F.2d 515, 523 n.10 (9th Cir. 1989).

[115]18 U.S.C.A. § 1030(g); *Sewell v. Bernardin*, 795 F.3d 337 (2d Cir. 2015) (holding claims by the plaintiff against her ex-boyfriend that were filed on January 2, 2014 time barred with respect to her AOL email account, where the plaintiff first found she could not log into her account on August 1, 2011, but not time barred with respect to access to her Facebook account, where she discovered that she could not log on, because her password had been altered, on February 24, 2012).

[116]*See* 47 U.S.C.A. § 230(c); *Holomaxx Technologies v. Microsoft Corp.*, 783 F. Supp. 2d 1097 (N.D. Cal. 2011) (dismissing as preempted by section 230(c)(2) (with leave to amend) plaintiff's claim under the Computer Fraud and Abuse Act); *Holomaxx Technologies v. Yahoo!, Inc.*, No. CV-10-4926-JF, 2011 WL 865794 (N.D. Cal. Mar. 11, 2011) (ruling the same way in dismissing Holomaxx's virtually identical complaint against Yahoo!); *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008) (granting judgment on the pleadings in favor of Comcast under the section 230(c)(2) on plaintiff's claims for violations of the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030, and unfair practices barred by the Illinois Consumer Fraud Act, arising out of Comcast's blocking email from e360, a bulk emailer, to Comcast subscribers); *see generally infra* § 37.05 (analyzing the CDA and the scope of its preemption in greater detail).

[117]*See, e.g.*, N.J. Stat. Ann. § 2A:38A–3; *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 277-78 (3d Cir. 2016) (affirming the district court's dismissal with prejudice of plaintiffs' claims under the New Jersey Computer Related Offenses Act (CROA), N.J. Stat. Ann. § 2A:38A–3, an anti-hacking statute, because plaintiffs could not "allege that they had been 'damaged in business or property,' as the plain text of the New Jersey Act requires"), *cert. denied*, 137 S. Ct. 624 (2017). New Jersey courts, the panel noted, construe the statute as requiring the same type of evidence of damage as that required by the federal Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030. *Id.* at 278.

trespass statutes.[118] Claims also potentially may be asserted under state unfair competition laws.[119] State statutes may afford relief not available under the CFAA, such as in a case where the $5,000 damage threshold cannot be met.[120]

5.07 DMCA and BOTS Act Claims

The Digital Millennium Copyright Act (DMCA) and Better Online Ticket Sales Act of 2016 (colloquially known as the BOTS Act) both proscribe circumvention of technological measures under different circumstances. The DMCA applies generally to circumvention of access and control mechanisms that protect copyrighted works.[1] The BOTS Act prohibits circumvention of a security measure, access control system, or other technological control or measure that an Internet site or service uses to enforce posted event ticket purchasing limits or to maintain the integrity of posted online ticket

---

[118] *See, e.g.*, Mo. Rev. Stat. §§ 537.525, 569.095 (the Missouri Computer Tampering Act, which prohibits, among other things, the knowing unauthorized receipt, use or disclosure of data and authorizes a civil action by the data owner); N.C. Gen. Stat. § 14-458 (making it illegal for any person "to use a computer or computer network without authority and with the intent" to undertake various alternative acts including removing, altering, erasing or disabling computer data, programs or software or making an unauthorized copy); *Spirax Sarco, Inc. v. SSI Engineering, Inc.*, 122 F. Supp. 3d 408, 417-18 (E.D.N.C. 2015) (holding that the plaintiff stated a claim under section 14-458(a) where it alleged that the defendant "intentionally used his Spirax-issued laptop to download vast quantities of computer files to his own media devices and Dropbox account, without authorization and in contravention of Spirax policies, and he also deleted vast quantities of computer files from the Spirax-issued laptop without authorization.").

[119] *See supra* § 5.04[2].

[120] *See, e.g.*, *Domain Name Commission Ltd v. DomainTools, LLC*, 449 F. Supp. 3d 1024, 1030-32 (W.D. Wash. 2020) (dismissing plaintiff's CFAA claim for scraping data because plaintiff could not meet the $5,000 damage threshold but holding that plaintiff stated a claim under Washington's Consumer Protection Act ("CPA"), Wash. Rev. Code Ann. § 19.86, where plaintiff alleged that defendant's efforts to circumvent the rate limiting and use restrictions plaintiff imposed to protect the data on its servers was "unfair or deceptive," that defendant engaged in these unfair acts in order to create and sell its products and services, that the public's interest is impacted because consumers are deprived of their privacy, and that plaintiff has incurred expenses and suffered injury to reputation and good will as a result).

[Section 5.07]

[1] *See* 17 U.S.C.A. §§ 1201 *et seq.*; *infra* § 5.07[1].

purchasing order rules.[2] The BOTS Act applies only to online ticket sales, whereas the DMCA generally applies to content protection and access control measures used to prevent copying of copyrighted works.

The DMCA also proscribes intentionally removing copyright management information (CMI) from copyrighted works, including potentially databases or the contents of a database, and using false CMI.[3]

5.07[1] DMCA Anti-Circumvention Provisions

The anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA) may provide remedies to a database owner where a third party attempts to circumvent measures intended to protect a copyrighted database or access to the database.[1] These provisions are analyzed in greater detail in section 4.21.

Section 1201(a) of the anti-circumvention provisions of the Digital Millennium Copyright Act, 17 U.S.C.A. § 1201(a), prohibits circumvention of a technological measure that effectively controls[2] access to a work protected by the Copyright Act. Among other things, something as simple as a password may qualify as an access control.[3] There is presently a circuit split over whether a claim may be stated for circumventing access controls that merely restrict access to unprotectable material.[4] Unlike a claim brought under the Copyright Act, fair use is not a defense to an anti-

---

[2] *See* 15 U.S.C.A. § 45c; *infra* § 5.07[3].

[3] *See* 17 U.S.C.A. § 1202; *infra*§ 5.07[2].

[Section 5.07[1]]

[1] 17 U.S.C.A. §§ 1201 *et seq*.

[2] *See, e.g.*, *Digital Drilling Data Systems, L.L.C. v. Petrolink Services, Inc.*, 965 F.3d 365, 375-77 (5th Cir. 2020) (affirming summary judgment for the defendant; "Although the USB dongle and Interface Process limited MWD companies' ability to make use of DataLogger, these measures did not control access to program's database itself, including its protected schema.").

[3] *See, e.g.*, *Synopsys, Inc. v. InnoGrit, Corp.*, Case No. 19-CV-02082-LHK, 2019 WL 4848387, at *8 (N.D. Cal. Oct. 1, 2019) ("a defendant's unauthorized use of license keys or passwords, as Synopsys has alleged, constitutes circumvention under Section 1201(a)(1)."); *infra* § 4.21[2][A].

[4] *See, e.g.*, *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 421 F.3d 1307 (Fed. Cir. 2005) (holding that defendant's circumventing encryption software to access error messages produced by plaintiff's maintenance, as part of his business of repairing

circumvention claim.[5]

There is thus a risk that circumventing access controls to scrape data could be actionable under section 1201(a). Where a violation is shown, the DMCA authorizes injunctive relief, recovery of attorneys' fees, and either actual damages or statutory damages of between $200 and $2,500 per act of circumvention (potentially trebled for repeat violations).[6] While this range is much lower than the range for statutory damages available for copyright infringement, statutory damages under the DMCA are awarded per violating act, not per work infringed (as under the Copyright Act). Thus, if a site is scraped repeatedly, the amount of statutory damages could be significant. And if a defendant is a repeat violator, the amount may be trebled.

Section 1201 also prohibits trafficking in devices that may be used to circumvent either access or copy control mechanisms.

Section 1201(a) protects against circumvention of access controls, while 1201(b) proscribes circumvention of technologies that protect against copying. Sections 1201(a)(2) and 1201(b)(1) collectively are referred to as anti-trafficking provisions. Section 1201(b)(1) addresses trafficking in technologies that circumvent technical measures that prevent copying. Section 1201(a)(2) prohibits trafficking in technologies that circumvent technological measures that effectively control access to protected works. Section 1201(a)(1), in turn, prohibits the actual circumvention of access controls. There is no corresponding prohibition on the actual circumvention of copy protection mechanisms, which may in some circumstances amount to a fair use under copyright law.

---

data libraries, did not violate section 1201 because the activities were protected by section 117 of the Copyright Act); *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004) (holding that the DMCA did not apply to garage door openers because section 1201 only prohibits forms of access that bear a reasonable relation to protections that the Copyright Act otherwise affords copyright owners), *cert. denied*, 544 U.S. 923 (2005). *But see MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 629 F.3d 928, 948-49, 952 (9th Cir. 2010) (disagreeing with this view and holding that the statute "created a distinct anti-circumvention right under § 1201(a) without an infringement nexus requirement."); *see generally infra* § 4.21[2][A].

[5]*See, e.g.*, *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443-59 (2d Cir. 2001); *infra* § 4.21[2][A].

[6]*See* 17 U.S.C.A. § 1201(c)(3)(A); *see generally infra* § 4.21[5].

There is, however, no fair use exception to the anti-circumvention provisions of the DMCA[7] (although the Copyright Office has issued rules creating certain statutory exceptions, which are revised every three years[8]).

One court characterized the elements necessary to state a DMCA claim as: (1) ownership of a valid copyright; (2) circumvention of a technological measure designed to protect the copyrighted material; (3) unauthorized access by third parties; (4) infringement because of the circumvention; and (5) the circumvention was achieved through software that the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.[9]

In *Ticketmaster LLC v. RMG Technologies, Inc.*,[10] the court ruled that Ticketmaster was likely to prevail on its claim under section 1201(a)(2) (trafficking in a device that circumvents technological measures that control access to a protected work) that the defendant violated the DMCA by offering a software tool that allowed its customers to circumvent technological measures, such as CAPTCHA,[11] employed by Ticketmaster to block automated access to its site. The court also found that Ticketmaster was likely to prevail on its claim under section 1201(b)(1) (for trafficking in a device

---

[7]*See, e.g.*, *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443-59 (2d Cir. 2001); *Disney Enterprises, Inc. v. VidAngel, Inc.*, 371 F. Supp. 3d 708, 715-16 (C.D. Cal. 2019); *see also, e.g.*, *Apple Inc. v. Corellium, LLC*, 510 F. Supp. 3d 1269, 1294-95 (S.D. Fla. 2020) ("Corellium's position that fair use is a defense to Apple's DMCA claim . . . would effectively render section 1201 meaningless. . . . [T]he Court finds that the better reading is that adopted by the *Corley* court. Therefore, Corellium may make fair use of iOS, but it is not absolved of potential liability for allegedly employing circumvention tools to unlawfully access iOS or elements of iOS."); *see generally supra* § 4.21 (addressing this issue in greater detail).

[8]*See supra* § 4.21[2][B].

[9]*Facebook, Inc. v. Power Ventures, Inc.*, 91 U.S.P.Q.2d 1430, 2009 WL 1299698 (N.D. Cal. May 11, 2009), *citing Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[10]*Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

[11]CAPTCHA (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a computer security program that is designed to distinguish between human users and computer programs, and thereby prevent automated devices from accessing a site.

that circumvents technological measures that protect the rights of a copyright owner in a work). The court reasoned that CAPTCHA both controls access to a protected work because a user could not proceed to copyright protected webpages without solving CAPTCHA and protects rights of a copyright owner because, by preventing automated access to the ticket purchase webpage, CAPTCHA prevents users from copying those pages.[12]

Similarly, in *Facebook, Inc. v. Power Ventures, Inc.*,[13] Judge Jeremy Fogel of the Northern District of California denied defendant's motion to dismiss plaintiff's DMCA claim, which was premised on the defendants allegedly circumventing technical measures intended to prevent them from accessing Facebook's website to copy user data in violation of the site's Terms of Use agreement. In so ruling, he rejected the defendants' argument that their access was not unauthorized because defendants merely provided a tool that their users (who were also Facebook users) used to access their own content. Judge Fogel concluded, however, that Facebook's Terms of Use agreement barred users from using automated programs to access the site.[14]

The court also rejected defendants' argument that there was no copyrighted work at issue because Facebook did not own a copyright to user content, which ultimately is the information that defendants' software sought to extract. Judge Fogel found that to access this data the defendants made a cached copy of the entire Facebook website and copied a user's entire Facebook profile page, simply to access the user's data. While Facebook did not own a copyright in individual user data, it likely did own one in the compilation of user data found on the Facebook site.

Although not discussed explicitly in the court's brief opinion, to effectively make such a claim, a site owner or service provider must establish that access was unauthorized (which in Facebook was based on exceeding the scope of permissible access, as set forth in the Terms of Use agreement) and that the defendant circumvented technical

---

[12]*Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096, 1111–12 (C.D. Cal. 2007).

[13]*Facebook, Inc. v. Power Ventures, Inc.*, 91 U.S.P.Q.2d 1430, 2009 WL 1299698 (N.D. Cal. May 11, 2009).

[14]*See supra* § 5.03[2] (discussing specific provisions of the Terms of Use agreement at issue in Facebook).

measures intended to block this access.

Other courts also have entered judgment for database and website owners based on the DMCA,[15] although no claim may be made absent circumvention.[16] Using software that ordinarily is only subject to an access control measure is not the same thing as establishing that the defendant in fact engaged in circumvention, as opposed to merely gaining access to it after someone else did so. "Because § 1201(a)(1) is targeted at circumvention, it does not apply to the use of copyrighted works *after* the technological measure has been circumvented."[17]

Where a company markets a product that allows users to employ bots to access a site (for example, to play an online game generating virtual goods or currency), liability could arise under the DMCA to the extent the program allows users to circumvent technological measures intended to defeat the use of bots or for breach of contract, tortious interference

---

[15]*See, e.g., DHI Group, Inc. v. Kent*, Civil Action H–16–1670, 2017 WL 4837730, at *5 (S.D. Tex. Oct. 26, 2017) (denying DHI's motion to dismiss Oilpro's DMCA claim where Oilpro alleged that it "had technological measures in place, including a robots.txt file, monitoring software, and firewall software, to prevent automated technologies from accessing the website" and DHI "circumvented these technological measures to access the Oilpro website and download material that was then published on [DHI's] own website."); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1055–57 (N.D. Cal. 2010) (entering a default judgment for violations of sections 1201(a)(2) and 1201(b)(1) and awarding $470,000 in statutory damages under the DMCA where the defendant marketed products that circumvented plaintiff's CAPTCHA software and telephone verification security measures).

[16]*See, e.g., Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 642–46 (E.D. Pa. 2007) (granting summary judgment for the defendants in a case where plaintiffs sued the law firm that previously had represented an opposing party in a trademark infringement suit, alleging that defendants obtained archived copies of its website from the Wayback Machine, www.Archive.org, where the copies were only accessible because of a computer malfunction that caused the Archive.org site to ignore the Robots.txt files on plaintiff's site that would otherwise have resulted in the archived pages being made publicly inaccessible; the defendants did not circumvent the Robots.txt file and plaintiff's inference that defendants should have known they were "not allowed to view the archived images via the Wayback Machine was both unreasonable and irrelevant" to the DMCA claim).

[17]*MGE UPS Systems, Inc. v. GE Consumer and Indus., Inc.*, 622 F.3d 361, 366 (5th Cir. 2010) (*en banc*) (affirming dismissal of plaintiff's claim; emphasis in original).

with contract or other grounds.[18]

There presently are circuit splits on a number of issues, including (as noted earlier) whether section 1201(a) created a new statutory anti-circumvention right distinct from infringement or whether circumvention of an access control is only actionable if it facilitates infringement. Under either view, the work accessed must be a copyrighted work to state a claim under section 1201(a). The difference is that according to the Ninth Circuit, sections 1201(a)(1) and 1201(a)(2) created "a new form of protection, i.e., the right to prevent circumvention of access controls, broadly to. . . copyrighted works[,]"[19] whereas the Federal Circuit requires a further showing of a nexus between the circumvention and infringement, which places circumvention undertaken to enable fair use or other noninfringing uses outside of section 1201(a)'s reach.[20]

Anti-circumvention case law is analyzed in substantially greater detail in section 4.21[2].

5.07[2] Removing, Altering or Falsifying Copyright Management Information

Removing, altering or falsifying copyright management information (CMI) is potentially actionable under section 1202 of the Digital Millennium Copyright Act.[1] Removing CMI or adding fake CMI may justify injunctive relief, actual dam-

---

[18] *See MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 629 F.3d 928 (9th Cir. 2011) (affirming entry of judgment for Blizzard under section 1201(a)(2), but reversing judgment on its copyright infringement and section 1201(b) claims and reversing based on disputed facts the entry of summary judgment on plaintiff's claim for tortious interference with the plaintiff's Terms of Use); *see also MDY Industries, LLC v. Blizzard Entertainment, Inc.*, No. CV-06-2555-PHX-DGC, 2011 WL 2533450 (D. Ariz. June 27, 2011) (declining to vacate the permanent injunction pursuant to section 1201(a)(2) on remand); *see generally infra* § 51.02[3] (analyzing the case in greater detail in the context of virtual goods and currency).

[19] *MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 629 F.3d 928, 945 (9th Cir. 2011).

[20] *See Storage Tech. Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 421 F.3d 1307, 1318-19 (Fed. Cir. 2005) (applying First Circuit law); *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178, 1192-1203 (Fed. Cir. 2004) (applying Seventh Circuit law), *cert. denied*, 544 U.S. 923 (2005).

[Section 5.07[2]]

[1] *See* 17 U.S.C.A. § 1202(c)(6); *see generally supra* § 4.21[3] (analyzing the statute in greater detail and discussing case law).

ages, or statutory damages of between $2,500 to $25,000 per violation.

Section 1202(a) prohibits any person from knowingly and with the intent to induce, enable, facilitate or conceal infringement,

(1) providing CMI that is false or
(2) distributing or importing for distribution CMI that is false.

Section 1202(b), in turn, prohibits anyone, without the authority of the copyright owner or the law, from

- intentionally removing or altering any CMI;
- distributing or importing for distribution CMI knowing that the CMI has been removed or altered without authority of the copyright owner or the law; or
- distributing, importing for distribution, or publicly performing works, copies of works, or phonorecords, knowing that CMI has been removed or altered without the authority of the copyright owner or the law,

knowing (or in the case of a civil suit pursuant to section 1203, "having reasonable ground to know") that it will induce, enable, facilitate or conceal copyright infringement.[2]

Absent knowledge, there can be no violation of section 1202.[3] At least two district courts further have held that a claim under 1202(b) must be premised on removal of CMI from the "body" or "area around" a work to violate the DMCA[4] and that a claim may not proceed if it is based merely on a general copyright notice appears on an entirely different webpage than the page where the work at issue appears.[5] The rationale for this rule is to prevent "a 'gotcha' system

---

[2]17 U.S.C.A. § 1202(b). Certain limited exceptions involving broadcast stations and cable systems are set forth in section 1202(e).

[3]*See Gordon v. Nextel Communications*, 345 F.3d 922, 926-27 (6th Cir. 2003) (affirming summary judgment for the defendant on plaintiff's claim under 1202(b)(3) where there was no evidence of that defendants knew that CMI had been removed or altered without the authority of the copyright owner).

[4]*Schiffer Publishing, Ltd. v. Chronicle Books, LLC*, No. 03 C 4962, 2004 WL 2583817, at *4, 14 (E.D. Pa. Nov.12, 2004) (finding no DMCA violation where a book contained 118 copyrighted photos with no CMI near them and the defendant merely had a general copyright notice on the whole book).

[5]*See Personal Keepsakes, Inc. v. Personalizationmall.com, Inc.*, No.

where a picture or piece of text has no CMI near it but the plaintiff relies on a general copyright notice buried elsewhere on the website."[6] As a practical matter, however, the requirement that a plaintiff establish knowledge or intent eliminates the risk of "gotcha" liability being imposed.

While a 1202(a) prohibits false CMI, section 1202(b) prohibits removal. To state a claim under section 1202(b) a plaintiff therefore must allege *removal*. Merely copying information into a different form (such as taking notes of an oral lecture and incorporating them into a note package)[7] does not amount to removal. Similarly, a claim for false CMI under section 1202(a) requires a showing that an alteration was made to an original work and may not be maintained where allegedly infringing material is merely incorporated into a new product with information that identifies the new product.[8] By contrast, where attribution information is replaced, a claim may be stated under section 1202(a) where a plaintiff can allege (a) knowledge that the CMI information is false, and (2) intent to induce, enable, facilitate or conceal an infringement of any right under Title 17.[9]

To constitute CMI, markings need not have been placed on

---

11 C 5177, 2012 WL 414803, at *7 (N.D. Ill. Feb. 8, 2012).

[6] *Personal Keepsakes, Inc. v. Personalizationmall.com, Inc.*, No. 11 C 5177, 2012 WL 414803, at *7 (N.D. Ill. Feb. 8, 2012). Judge Virginia M. Kendall premised this ruling on the definition of CMI, which requires that CMI be *conveyed* with a copyrighted work. *See id.*

[7] *See Faulkner Press, LLC v. Class Notes, LLC*, 756 F. Supp. 2d 1352, 1359 (N.D. Fla. 2010).

[8] *See Faulkner Press, LLC v. Class Notes, LLC*, 756 F. Supp. 2d 1352, 1359-60 (N.D. Fla. 2010) (holding that the defendant did not add false CMI by printing "Einstein's Notes ©" on its note packages where the note package was a different work from Class Notes even if, as the plaintiff alleged, it included material from the plaintiff's work because "[n]o alteration was made to Dr. Moulton's product or original work, so there was no violation of the DMCA.").

[9] *See, e.g.*, *Agence France Presse v. Morel*, 769 F. Supp. 2d 295, 304-05 (S.D.N.Y. 2011) (holding that the plaintiff pled a claim for falsification under section 1202(a) by alleging that Agence France Presse labeled his photographs with the credit lines "AFP/Getty/Daniel Morel" and "AFP/Getty/Lisandro Suero" which the plaintiff alleged were false and intended to facilitate infringement); *Ward v. National Geographic Society*, 208 F. Supp. 2d 429, 449 (S.D.N.Y. 2002) (granting summary judgment for the defendant because a defendant's knowledge may not be imputed).

a work by the copyright owner itself.[10]

On the other hand, merely because a copyright owner's name was removed does not mean that a section 1202 claim will be viable or that the name constituted CMI. In *Fischer v. Forrest*,[11] for example, the Second Circuit affirmed summary judgment for the defendant in a case where the defendant had closely copied plaintiff's copyrighted advertisement, but replaced plaintiff's name with its own. The appellate court explained that "[w]hile an author's name can constitute CMI, not every mention of the name does. Here, . . . what was removed was not Fischer's name as the copyright holder of the advertising text, but 'Fischer's' insofar as it was a part of the actual product's name."[12]

According to the Second Circuit, section 1202(a) (which proscribes false CMI) creates a "double scienter requirement" requiring that a plaintiff prove or "plausibly allege that defendant knowingly provided false copyright management information *and* that the defendant did so with the intent to induce, enable, facilitate, or conceal an infringement."[13]

A claim under any of the three subparts of section 1202(b) (involving alteration or removal of CMI) requires an affirmative showing that a defendant knew that the prohibited act

---

[10]*See, e.g.*, *Mango v. Buzzfeed, Inc.,* 970 F.3d 167, 171 n.1 (2d Cir. 2020) ("The DMCA, by its express terms, contains no requirement that a copyright owner personally affix CMI."); *GC2 Inc. v. Int'l Game Technology*, 391 F. Supp. 3d 828, 845 (N.D. Ill. 2019) ("Nowhere does the text of section 1202 suggest that removal of copyright management information is only a violation if that information was placed on the copyrighted materials by the plaintiff itself. Such a reading would lead to the absurd result where a copyright owner who contracts with another entity to manufacture their products—and in the process to affix copyright management information—could not avail itself of the DMCA's removal provisions.").

[11]*Fischer v. Forrest*, 968 F.3d 216 (2d Cir. 2020), *cert. denied*, __ S. Ct. __, 2021 WL 5167839 (2021).

[12]*Fischer v. Forrest*, 968 F.3d 216, 223 (2d Cir. 2020), *cert. denied*, __ S. Ct. __, 2021 WL 5167839 (2021). The appellate court elaborated that

> "Fischer's" is part of a product name; it is not a reference to "James H. Fischer" as the owner of a copyrighted text. Nor is the name "[t]he title and other information identifying the work" or the "[t]he name of, and other identifying information about, the author of the work" as required by the statute. *See* 17 U.S.C. § 1202(c)(1)-(3).

Id.

[13]*Krechmer v. Tantaros*, 747 F. App'x 6, 9-10 (2d Cir. 2018) (affirming dismissal of plaintiff's section 1202(a) claim).

would "induce, enable, facilitate, or conceal" infringement.[14]

As with a claim under section 1202(a), the Second Circuit has held that "[s]ection 1202(b)(3) contains a so-called 'double-scienter' requirement: the defendant who distributed improperly attributed copyrighted material must have actual knowledge that CMI 'has been removed or altered without authority of the copyright owner or the law,' as well as actual or constructive knowledge that such distribution 'will induce, enable, facilitate, or conceal an infringement.' "[15] To state a claim, the Second Circuit has held that a plaintiff must prove: (1) the existence of CMI in connection with a copyrighted work; and (2) that a defendant "distribute[d] . . . works [or] copies of works"; (3) while "knowing that [CMI] has been removed or altered without authority of the copyright owner or the law"; and (4) while "knowing, or . . . having reasonable grounds to know" that such distribution "will induce, enable, facilitate, or conceal an infringement."[16]

Courts disagree about whether *Copyright Management Information* must involve technical measures of automated systems, which is suggested by the legislative history. As analyzed in section 4.21[3], the trend is to construe CMI broadly based on the plain terms of the statute, rather than more narrowly based on legislative history.

In *Associated Press v. All Headline News Corp.*,[17] for example, a court in the Southern District of New York held that the plaintiff had stated a claim under 17 U.S.C.A. § 1202 where it alleged that defendants took Associated Press articles from the Internet and removed information that identified the AP as the owner and author, before reproducing them on their website. In so ruling, however, the court disagreed with courts in New Jersey and Califor-

---

[14]*Stevens v. Corelogic, Inc.,* 899 F.3d 666, 673 (9th Cir. 2018) (affirming summary judgment for the defendant; both sections 1202(b)(2) and 1202(b)(3) "require the defendant to possess the mental state of knowing, or having a reasonable basis to know, that his actions 'will induce, enable, facilitate, or conceal' infringement.").

[15]*Mango v. Buzzfeed, Inc.,* 970 F.3d 167, 171 (2d Cir. 2020) (affirming judgment for the plaintiff, following a bench trial); *see also Zuma Press, Inc. v. Getty Images (US), Inc.*, 845 F. App'x 54, 57-58 (2d Cir. 2021) (affirming summary judgment for Getty Images on plaintiff's section 1202(b)(3) claim).

[16]*Mango v. Buzzfeed, Inc.,* 970 F.3d 167, 171 (2d Cir. 2020).

[17]*Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454 (S.D.N.Y. 2009).

nia that had held that to state a claim under section 1202 a plaintiff must alter, remove or falsify technological measures of automated systems, which the court in *All Headline News* criticized as being based on legislative history rather than the plain text of the statute.

Following *All Headline News*, the court in *Cable v. Agence France Press*[18] denied the defendant's motion to dismiss, holding that the plaintiff's name and a link ("Photos © 2009 wayne cable, selfmadephoto.com"), which allegedly had been removed from plaintiff's photos before they were included without authorization in the defendant's photo database, constituted *copyright management information* "in the absence of evidence to the contrary, which may be considered in the context of future dispositive motions . . . ."

A party's copying and reuse of content from a database with CMI removed potentially could violate section 1202. If CMI is not removed, however, it potentially could lead to exposure under the Lanham Act to the extent that its inclusion is likely to cause confusion or dilution.[19]

Case law on removal, alteration and falsification of Copyright Management Information is analyzed in greater detail in section 4.21[3].

5.07[3] BOTS Act Anticircumvention

The Better Online Ticket Sales Act of 2016 (colloquially known as the BOTS Act)[1] makes it unlawful to "circumvent a security measure, access control system, or other technological control or measure on an Internet website or online service that is used by the ticket issuer[2] to enforce posted

---

[18]*Cable v. Agence France Presse*, 728 F. Supp. 2d 977, 981 (N.D. Ill. 2010).

[19]*See infra* § 5.08.

[Section 5.07[3]]

[1]*See* 15 U.S.C.A. § 45c.

[2]While the definition of *ticket issuer* was not codified, a note to the statute includes the definition contained in the law enacted by Congress, which is what the FTC will follow. *Ticket issuer* means

> any person who makes event tickets available, directly or indirectly, to the general public, and may include—
>
> (A) the operator of the venue;
>
> (B) the sponsor or promoter of an event;

event[3] ticket[4] purchasing limits or to maintain the integrity of posted online ticket purchasing order rules . . . ."[5] The Act also makes it unlawful "to sell or offer to sell any event ticket in interstate commerce" obtained in violation of this prohibition if the person selling or offering to sell the ticket "participated directly in or had the ability to control the conduct"[6] or "knew or should have known that the event ticket was acquired in violation of" this prohibition.[7]

The Act creates exceptions allowing a person to create or use any computer software or system "to investigate, or further the enforcement or defense, of any alleged violation of this section or other statute or regulation"[8] or "to engage in research necessary to identify and analyze flaws and vulner-

---

(C) a sports team participating in an event or a league whose teams are participating in an event;

(D) a theater company, musical group, or similar participant in an event; and

(E) an agent for any such person."

15 U.S.C.A. § 45c note; Pub. L. 114–274 § 3, 130 Stat. 1403 (Dec. 14, 2016).

[3]While the definition of *event* was not codified, a note to the statute includes the definition contained in the law enacted by Congress, which is what the FTC will follow. *Event* means "any concert, theatrical performance, sporting event, show, or similarly scheduled activity, taking place in a venue with a seating or attendance capacity exceeding 200 persons that—(A) is open to the general public; and (B) is promoted, advertised, or marketed in interstate commerce or for which event tickets are generally sold or distributed in interstate commerce." 15 U.S.C.A. § 45c note; Pub. L. 114–274 § 3, 130 Stat. 1403 (Dec. 14, 2016).

[4]While the definition of *event ticket* was not codified, a note to the statute includes the definition contained in the law enacted by Congress, which is what the FTC will follow. The term *event ticket* means "any physical, electronic, or other form of a certificate, document, voucher, token, or other evidence indicating that the bearer, possessor, or person entitled to possession through purchase or otherwise has— (A) a right, privilege, or license to enter an event venue or occupy a particular seat or area in an event venue with respect to one or more events; or (B) an entitlement to purchase such a right, privilege, or license with respect to one or more future events." 15 U.S.C.A. § 45c note; Pub. L. 114–274 § 3, 130 Stat. 1403 (Dec. 14, 2016).

In the view of the FTC, an *event ticket* does not include online travel tickets for bus, train or airline travel. *See* FTC, *BOTS Act: That's The Ticket!* (Apr. 7, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/04/bots-act-thats-ticket (Apr. 13, 2017 5:12 PM Comment).

[5]15 U.S.C.A. § 45c(a)(1)(A).

[6]15 U.S.C.A. § 45c(a)(1)(B)(i).

[7]15 U.S.C.A. § 45c(a)(1)(B)(ii).

[8]15 U.S.C.A. § 45c(a)(2)(A).

abilities of measures, systems, or controls . . . if these research activities are conducted to advance the state of knowledge in the field of computer system security or to assist in the development of computer security product."[9]

Violations of the BOTS Act may be enforced by the Federal Trade Commission as an unfair or deceptive practice,[10] pursuant to the Federal Trade Commission Act,[11] or by State Attorneys General.[12]

The BOTS Act neither authorizes a private cause of action nor expressly prohibits one. The Act preempts certain enforcement by State Attorneys General[13] but does not purport to create or preempt civil remedies. It is therefore possible that a violation of the BOTS Act, while not independently actionable, could form the basis of a state law unfair competition claim in those states, such as California, that allow claims to be brought for violations under statutes that do not afford a private cause of action[14] (unless it were determined that Congress sought to occupy the field, resulting in "field preemption" of state law claims[15]).

---

[9]15 U.S.C.A. § 45c(a)(2)(B).

[10]15 U.S.C.A. § 45c(b)(1).

[11]15 U.S.C.A. §§ 45, 46; *see generally infra* § 25.02 (analyzing FTC jurisdiction and regulation of Internet and mobile activities).

[12]15 U.S.C.A. § 45c(c).

[13]*See* 15 U.S.C.A. § 45c(c)(4).

[14]*See, e.g.,* Cal. Bus. & Prof. §§ 17200 *et seq.* Section 17200 "borrows" violations from other laws by making them independently actionable as unfair competitive practices. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143–45, 131 Cal. Rptr. 2d 29 (Cal. 2003). Under section 17200, "[u]nlawful acts are 'anything that can properly be called a business practice and that at the same time is forbidden by law . . . be it civil, criminal, federal, state, or municipal, statutory, regulatory, or court-made,' where court-made law is, 'for example a violation of a prior court order.' " *Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1151–52 (9th Cir. 2008) (citations omitted); *see generally infra* §§ 6.12[6] (analyzing unfair practices laws in greater detail), 25.04[3] (addressing unfair competition in connection with an overview of consumer protection laws).

[15]States "are precluded from regulating conduct in a field that Congress, acting within its proper authority, has determined must be regulated by its exclusive governance." *Arizona v. United States,* 567 U.S. 387, 399 (2012). Preemption may be express, as it is in some statutes, or "[t]he intent to displace state law altogether can be inferred from a framework of regulation 'so pervasive . . . that Congress left no room for the States to supplement it' or where there is a 'federal interest . . . so dominant that the federal system will be assumed to preclude enforce-

5.08 Lanham Act Remedies

Where material copied from a database includes logos or other branding, a claim potentially may be asserted under the Lanham Act.[1] Often, however, a screen scraper is smart enough to only post unprotectable data, not branding that may have been included with the data. Likewise, merely including a company's name may be insufficient if the name isn't used in a trademark sense.[2] If scraped material is

---

ment of state laws on the same subject.' " *Id., quoting Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947). Given that Congress expressly chose to include a preemption provision applicable to State Attorneys General actions but not to civil claims, an argument may be advanced that Congress did not intend to occupy the field (unless there is a contradictory intention expressed in the legislative history).

[Section 5.08]

[1]*See* 15 U.S.C.A. § 1125(a); *see generally infra* § 6.12. For example, in *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1058–60 (N.D. Cal. 2010), the court entered a default judgment for trademark infringement under the Lanham Act and California law based on the defendants' display of the Craigslist mark in the text and in the headings of sponsored links advertising products to automate the process of posting listings to Craigslist, in advertising their products and on their website.

In *Health Grades, Inc. v. Robert Wood Johnson University Hosp., Inc.*, 634 F. Supp. 2d 1226, 1239–43 (D. Colo. 2009), the court denied the defendant's motion to dismiss plaintiff's trademark infringement claim where the issues of likelihood of confusion and nominative fair use (considered in the context of likelihood of confusion) presented factual issues that could not be resolved on a motion to dismiss. In that case, Health Grades sued a hospital alleging that it breached its click-through license agreement with the plaintiff by commercially reproducing, modifying and/or distributing its healthcare provider award and ranking information from plaintiff's website, including its trademarks, in press releases and other marketing materials.

Similarly, in *Southwest Airlines Co. v. Roundpipe, LLC*, 375 F. Supp. 3d 687, 706 (N.D. Tex. 2019), the court denied defendants' motion to dismiss claims for unfair competition, trademark infringement, and trademark dilution, where Southwest alleged that defendants used automated tools to scrape information from its website which it alleged was reproduced without authorization on defendants' www.SWMonkey.com website, tarnishing its marks and causing consumer confusion.

Needless to say, it may be easier to allege than prove infringement or dilution or negate fair use or non-trademark use arguments in cases where data or information is scraped from a site or service. The elements of claims for infringement, dilution, and unfair competition, and the grounds for establishing fair or permissible use are analyzed extensively in chapter 6.

[2]*See, e.g.*, *Alan Ross Machinery Corp. v. Machinio Corp.*, No. 17-cv-3569, 2018 WL 3344364, at *3 (N.D. Ill. July 9, 2018) (dismissing Alan

entitled to copyright protection and includes copyright management information (CMI), however, removing the information to avoid exposure under the Lanham Act potentially could result in liability for removing CMI under the Digital Millennium Copyright Act.[3]

Where a database owner's marks are displayed on a competitor's site, the database owner potentially may maintain a claim for trademark infringement, unfair competition, false designation of origin or passing off, provided likelihood of confusion may be shown.[4] If the association of a database owner's marks with a given site tarnishes or blurs the mark, and if the mark may qualify as "famous," a claim also may be maintained for dilution.[5] If the site merely identifies the database owner, the reference may be a nominative fair use.[6] Where the fact of display is a function of fair use copying, the display also could be deemed a fair use in limited circumstances.[7]

Ross Machinery's Lanham Act claim, in a case alleging that Machinio scraped sales listings of industrial machinery from Alan Ross's website and duplicated those listings on its website, where Alan Ross did not allege that the reference to "Alan Ross Machinery" on the listings on Machinio's website were used in a trademark sense and did not allege sufficient facts to support the assertion that the "click to contact seller" button next to every listing would confuse consumers).

[3]17 U.S.C.A. § 1202; *supra* § 5.07[2] (database-related DMCA claims); *see generally supra* § 4.21[3] (analyzing the statute in depth).

[4]*See infra* chapter 6.

[5]*See infra* § 6.11.

[6]The nominative fair use defense permits certain uses of a trademark to refer to the trademarked product. *See infra* § 6.14[3]. For example, in *Comparion Medical Analytics, Inc. v. Prime Healthcare Services, Inc.*, Case No. 2:14-CV-3448 SVW (MANx), 2015 WL 12746228, at *1-5 (C.D. Cal. Apr. 14, 2015), the court entered summary judgment for the defendant on claims for trademark infringement and unfair competition under the Lanham Act and common law unfair competition based on nominative fair use, in a case brought by a company that "grants to hospitals awards, and then sells them the right to publicize the awards . . . ," where the plaintiff gave the defendant "numerous awards . . . [and] then sued Prime for posting news of the awards on its website . . ." without a license to do so.

[7]*See, e.g., Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992) (Sega marks displayed because they were embedded in code needed to be used to make Accolade's game compatible with Sony's player that used a proprietary format); *Health Grades, Inc. v. Robert Wood Johnson University Hosp., Inc.*, 634 F. Supp. 2d 1226, 1239–43 (D. Colo. 2009) (denying defendant's motion to dismiss where the plaintiff's marks were used in connection with a description of the defendant's ranking and

Where branding information or credits are edited out of material from a factual database or other compilation that is unprotectable, the database owner will not be permitted to maintain a Lanham Act claim for what amounts to a disguised claim for copyright (which, if actionable, must be brought under the Copyright Act, not the Lanham Act).[8] Where the material is protectable, however, a claim for reverse passing off potentially could be maintained.[9]

---

the awards it received from the plaintiff, where the court held that nominative fair use was an element of likelihood of confusion, which the plaintiff was required to prove in order to prevail); *see generally infra* §§ 6.12[3][C], 6.14.

[8]*See Dastar Corp. v. Twentieth Century Fox Film Corp.*, 539 U.S. 23 (2003); *see also*, *e.g., General Universal Systems, Inc. v. Lee*, 379 F.3d 131, 148–49 (5th Cir. 2004) (holding a software developer/licensor's reverse palming off claim preempted where it rested on the defendant's copying ideas, concepts, structures and sequences embodied in his copyrighted work, rather than palming off tangible copies); *Phoenix Entertainment Partners, LLC v. Rumsey*, 829 F.3d 817, 827-31 (7th Cir. 2016) (holding, on different facts from Dastar, that plaintiff's passing off claim for copying digital karaoke music files was preempted where the claim was directed at the creative content contained in the file); *Slep-Tone Entertainment Corp. v. Wired for Sound Karaoke & DJ Services, LLC*, 845 F.3d 1246 (9th Cir. 2017) (affirming dismissal under *Dastar* of plaintiff's trademark and trade dress claims as disguised claims alleging copying; following the Seventh Circuit's decision in *Rumsey*); *Citizens Information Associates, LLC v. Justmugshots.com*, Civil No. 1-12-CV-573-LY, 2013 WL 12076563, at *2-3 (W.D. Tex. Feb. 26, 2013) (dismissing the Lanham Act reverse passing off claim of the owner of BustedMugshots.com, which aggregated publicly available arrest records on its website, brought against JustMugShots.com, which repeatedly scraped its database and reprinted images from BustedMugshots.com on JustMugShots.com with the BustedMugshots.com logo obscured, as precluded by *Dastar*); *infra* § 6.12[1] (analyzing *Dastar*). *But see Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 935–36 (E.D. Va. 2010) (denying defendant's motion to dismiss a database owner's reverse passing off claim brought against a screen scraper to the extent that the plaintiff "does not assert that Eventbrite has passed off its ideas as its own, but rather than Eventbrite has re-branded and re-packaged its product (the CSN venue database) and sold it as its own."); *Cable v. Agence France Presse*, 728 F. Supp. 2d 977, 981 (N.D. Ill. 2010) (denying defendant's motion to dismiss where the plaintiff alleged that Agence France Presse took plaintiff's photos and repackaged them as its own in its own database, without revision); *Experian Marketing Solutions, Inc. v. U.S. Data Corp.*, No. 8:09cv24, 2009 WL 2902957 (D. Neb. Sept. 9, 2009) (holding that plaintiff's claim, involving an unauthorized copy of consumer data files, was not preempted because the database constituted a tangible good); *see generally infra* § 6.12[1] (analyzing case law).

[9]*See* 15 U.S.C.A. § 1125(a); *see generally infra* § 6.12.

In *Register.com, Inc. v. Verio, Inc.*,[10] the Second Circuit declined in part to rule as moot and reversed in part the lower court's holding that the plaintiff was likely to prevail on its Lanham Act claims. In that case, Verio had used bots to repeatedly copy from Register.com's website the WHOIS database (which lists the contact information for all domain name registrants in Top Level Domains for which *Register.com* acts as a registrar).[11] Verio used this information to contact new registrants soliciting their interest in services that it offered in competition with *Register.com* and its co-brand and private label partners. The court ruled that the portion of the injunction barring Verio from using Register.com's marks was moot because Verio had already agreed not to use Register.com's marks any longer and *Register.com* had agreed to modify the preliminary injunction to delete this part of the order. The other aspect of the preliminary injunction barred the phrasing of solicitations that the district court found misleading but which did not include any reference to *Register.com* or its marks, and which the Second Circuit therefore found was neither false nor misleading.[12]

In *Facebook, Inc. v. Power Ventures, Inc.*,[13] the court denied defendant's motion to dismiss plaintiff's Lanham Act claim where the plaintiff alleged that the defendants—operators of a website that used screen scraping tools to allow users to view email and social network accounts from a single location—sent Facebook users a screen shot advertising its service, which displayed Facebook's mark and appeared to have originated with or have been endorsed by Facebook.

In *Associated Press v. All Headline News Corp.*,[14] the court granted the defendants' motion to dismiss plaintiff's Lanham Act claims, in a case where the plaintiff alleged that defendants copied AP breaking news reports and reprinted

---

[10] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004).

[11] The WHOIS database and the roles of domain name registries and registrars are described in detail in chapter 7.

[12] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 440–43 (2d Cir. 2004). The telemarketing script referred to the person's recent registration of a domain name but did not name Register.com and included the truthful representation that the caller worked for Verio.

[13] *Facebook, Inc. v. Power Ventures, Inc.*, 91 U.S.P.Q.2d 1430, 2009 WL 1299698 (N.D. Cal. May 11, 2009).

[14] *Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454 (S.D.N.Y. 2009).

its news stories on their All Headline News (AHN) website, either as AP reports or AHN content. In rejecting plaintiff's conclusory allegations, Judge Castel wrote that "trademark law 'generally does not prevent one who trades a branded product from accurately describing it by its brand name, so long as the trader does not create confusion by implying an affiliation with the owner of the product.' "[15] Likewise, Judge Castel dismissed AP's false advertising claim, concluding that AHN's description of its site as a "news service" even though AHN did not do any original news reporting was not actionable because the term "news service" did not lend itself to absolute criteria and defendants' characterization of their service appeared to be permissible puffery.[16] The court denied defendants' motion to dismiss AP's state law unfair competition claim based on passing off, however, finding that the plaintiff had stated a claim by alleging that AHN passed off AP content as its own.[17]

By contrast, in *Cable v. Agence France Press*,[18] the court denied defendants' motion to dismiss plaintiff's reverse passing off claim (as well as its copyright management information claim under the DMCA)[19] where the plaintiff alleged that Agence France Press removed his name and copyright notice and the link to his website ("Photos © 2009 wayne cable, selfmadephoto.com") and republished his photos in its online photo database, ImageForum.[20]

Where a party copies material without attribution but modifies it in some way, a reverse passing off claim may not be brought.[21] Where attribution along with copyright management information is removed, however, a database

---

[15]*Associated Press v. All Headline News Corp.*, 608 F. Supp. 2d 454, 462 (S.D.N.Y. 2009), *quoting Dow Jones & Company, Inc. v. International Securities Exchange, Inc.*, 451 F.3d 295, 308 (2d Cir. 2006) (quotation marks omitted).

[16]608 F. Supp. 2d at 463; *see generally infra* § 6.12[5] (advertising, including puffery).

[17]608 F. Supp. 2d at 464.

[18]*Cable v. Agence France Presse*, 728 F. Supp. 2d 977 (N.D. Ill. 2010).

[19]17 U.S.C.A. § 1202; *see supra* §§ 5.07[2], 4.21.

[20]For further discussion of this aspect of the case, *see infra* § 6.12[2].

[21]*Dastar Corp. v. Twentieth Century Fox Film Corp.*, 539 U.S. 23 (2003); *see generally infra* § 6.12.

owner may be able to maintain a claim under the DMCA.[22]

In addition to claims under the Lanham Act, database owners may be able to assert equivalent claims for trademark infringement, dilution, false designation of origin, false advertising, passing off or unfair competition under state law.[23]

Except for dilution and certain false advertising claims, to prevail under the Lanham Act, a plaintiff must establish likelihood of confusion.[24] Mere copying is not actionable. Thus, while the Lanham Act may provide remedies in certain cases where material from a database is republished elsewhere, it does not proscribe access to data or copying.

5.09 Trade Secret Protection

Most commercially available databases typically are not treated as trade secrets. Needless to say, where public records in the public domain are posted on a publicly accessible website, scraping the records from a database does not amount to trade secret misappropriation.[1] Where the contents of a database constitute trade secrets, however, a database owner potentially may seek injunctive relief and damages for trade secret misappropriation provided the defendant in fact misappropriated the data and did not merely obtain it lawfully from a third party (in some jurisdictions, without knowledge that the material is a trade secret). Assuming that the contents of the database qualify for trade secret protection and are adequately protected as such, a database owner potentially could state a claim.[2] Misappropriation of trade secret claims generally are not preempted

---

[22]17 U.S.C.A. § 1202; *see generally supra* § 5.07[2].

[23]*See infra* §§ 6.04 (state trademarks), 6.11[7] (state law dilution), 6.12[6] (unfair competition); *supra* § 5.04 (misappropriation and unfair competition).

[24]*See infra* §§ 6.08, 6.11, 6.12[5].

[Section 5.09]

[1]*See, e.g.*, *Citizens Information Associates, LLC v. Justmugshots.com*, Civil No. 1-12-CV-573-LY, 2013 WL 12076563, at *3 (W.D. Tex. Feb. 26, 2013) (dismissing BustedMugshots.com's trade secret misappropriation claim where the plaintiff aggregated millions of publicly available arrest records on its website, which had been scraped by a competitor, JustMugShots.com, because the records scraped were not secret and "the fact that the underlying data is public domain information subjects Citizens's claims to preemption under the Copyright Act.").

[2]*See, e.g.*, *Compulife Software Inc. v. Newman*, 959 F.3d 1288,

so long as an extra element—such as misappropriation or

1312-15 (11th Cir. 2020) (remanding the case for further consideration of whether the defendants' access to Compulife's proprietary Transformative Database for generating insurance industry quotes constituted misappropriation by improper means (by use or acquisition); "Even granting that individual quotes themselves are not entitled to protection as trade secrets, the magistrate judge failed to consider the important possibility that so much of the Transformative Database was taken—in a bit-by-bit fashion—that a protected portion of the trade secret was acquired. The magistrate judge was correct to conclude that the scraped quotes 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. . . . Nor does the fact that the defendants took the quotes from a publicly accessible site 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."); *Compulife Software, Inc. v. Rutstein*, Case Nos. 9:16-CV-80808-REINHART, 9:16-CV-81942-REINHART, 2021 WL 3713173, at *19-21 (S.D. Fla. July 12, 2021) (entering judgment for Compulife on its Defend Trade Secrets Act and Florida Uniform Trade Secrets Act claims and holding defendants jointly and severally liable for $368,451.71 in damages (plus prejudgment interest), on remand, following a bench trial, based on the findings that Rutstein intentionally misled Compulife in August 2011, which directly resulted in his acquisition of Compulife's Transformative Database without Compulife's permission, in light of the Eleventh Circuit's finding that the database was protected as a trade secret, and that by "using a robot to hack the Term4Sale website, Defendants intentionally sought to acquire Compulife's trade secrets through improper means. Defendants' subsequent use of the Term4Sale 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."); *Physicians Interactive v. Lathian Systems, Inc*., No. CA 03-1193-A, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003) (enjoining defendants in a case where a Lathian employee secretly hacked Physicians Interactive's website and stole its confidential customer lists and computer software code, holding that "[t]here can be no doubt that the use of a computer software robot to hack into a computer system and to take or copy proprietary information is an improper means to obtain a trade secret, and thus is misappropriation under the VUTSA . . ."); *see generally infra* chapter 10.

In *Compulife,* the Eleventh Circuit and district court had held that "the trade-secret owner's 'failure to place a usage restriction on its website' did not automatically render the hacking proper." 2021 WL 3713173, at *21, *quoting* 959 F.3d at 1315. While this is undoubtedly true as a general proposition, it may go to the question of whether a trade secret owner

breach of a duty or trust—is alleged.[3]

If the content of a database is a trade secret, other state law claims potentially may be preempted in states that have enacted section 7 of the Uniform Trade Secrets Act.[4] Section 7 preempts conflicting tort, restitutionary, and other state laws providing civil remedies for misappropriation of a trade secret but does not preempt contractual remedies, whether or not based on misappropriation, and other civil remedies that are not based on misappropriation of a trade secret.[5] A copy of the UTSA is reprinted in the Appendix to chapter 10.

By contrast, a claim brought under the federal Defend

---

adequately protected its database as a trade secret. *See generally infra* chapter 10.

[3]*See, e.g., Dun & Bradstreet Software Services, Inc. v. Grace Consulting, Inc.*, 307 F.3d 197, 218 (3d Cir. 2002) (holding that a misappropriation claim based on breach of a duty or trust would not be preempted, while one based solely on copying would be preempted), *cert. denied*, 538 U.S. 1032 (2003); *Huckshold v. HSSL, LLC*, 344 F. Supp. 2d 1203 (E.D. Mo. 2004) (holding trade secret misappropriation and breach of contract claims not preempted where the plaintiff alleged that the defendant owed a duty to protect the confidentiality of plaintiffs' trade secrets and breached its contract by allowing a third party to copy the software in violation of their agreement (and was not merely a claim that the defendant itself copied the software), which thus involved an extra element, but finding plaintiff's tortious interference claim preempted where the only element needed to be shown to establish liability was copying); *see generally supra* § 4.18[1] (analyzing copyright preemption).

[4]As of October 2019, 48 states—every state except New York and North Carolina—as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had adopted a version of the Uniform Trade Secrets Act (UTSA). *See infra* § 10.02.

[5]UTSA § 7; *infra* § 10.17 (addressing UTSA preemption and analyzing cases construing section 7). A copy of the UTSA is reprinted in the appendix to chapter 10. Section 7 preemption—in some of the jurisdictions where it has been enacted into state law—preempts claims regardless of whether the underlying information is a trade secret, and may have particular application to claims involving business information and data. *See, e.g.*, *Heller v. Cepia, LLC*, No. C 11–01146 JSW, 2012 WL 13572, at *7 (N.D. Cal., Jan. 4, 2012) (dismissing claims for common law misappropriation, conversion, unjust enrichment, and trespass to chattels, because these claims, "premised on the wrongful taking and use of confidential business and proprietary information, regardless of whether such information constitutes trade secrets, are superseded by the CUTSA."); *see generally infra* § 10.17 (discussing conflicting lines of cases on whether a claim is preempted even if based on information that may not be protectable as a trade secret).

Trade Secrets Act (DTSA)[6] would not preempt other state claims that may be brought in addition to or instead of a claim under the DTSA.[7] It likewise does not limit the availability of remedies under other federal statutes,[8] such as the Computer Fraud and Abuse Act.[9]

Claims asserted against an interactive computer service provider for merely hosting database content alleged to incorporate trade secrets (as opposed to direct conduct by the site or service itself) may be preempted by the Good Samaritan exemption of the Telecommunications Act of 1996, also known as the Communications Decency Act, at least in the Ninth Circuit[10] for state law claims, and generally under the DTSA.

Claims for trade secret misappropriation are analyzed in chapter 10.

5.10 EU Database Directive

5.10[1] Overview

The European Parliament and the Council of the European Union enacted the EU Database Directive in 1996, which compels member states to afford fifteen-year *sui generis* protection for databases where there has been "qualitatively and/or quantitatively a substantial investment in either the

---

[6]18 U.S.C.A. §§ 1830 to 1839; *see generally infra* § 10.12[2].

[7]18 U.S.C.A. § 1838. That section states that except as set forth in section 1833(b) (which provides immunity from liability for the confidential disclosure of a trade secret to the government or an attorney for the purpose of reporting a violation of law, in a court filing under seal or in connection with an anti-retaliation lawsuit, provided the material is filed under seal and is not disclosed except pursuant to court order), 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, or to affect the otherwise lawful disclosure of information by any Government employee under . . ." the Freedom of Information Act, 5 U.S.C.A. § 552. *See* 18 U.S.C.A. § 1838; H.R. Rep. 114-529, 114th Cong. 2d Sess. 5 (2016) (stating that the DTSA does not preempt variations of the UTSA enacted in 48 states but "offers a complementary Federal remedy . . . .").

[8]See 18 U.S.C.A. § 1838; *see generally infra* § 10.12[2].

[9]18 U.S.C.A. § 1030; *see generally infra* § 44.08.

[10]47 U.S.C.A. § 230(c); *see generally infra* § 37.05[5][B].

obtaining, verification, or presentation of the contents."[1] A database is defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means."[2]

Rights to the *sui generis* protection created by the Directive are granted based on the location of the owner or author of the work, not the location where it was created. As discussed in subsection 5.10[3] below, the Directive potentially allows database makers or rights holders to extend protection indefinitely.

Sui generis rights are granted in addition to copyright protection, which may be available to database authors within the European Union based on original selection or arrangement.[3] Even under EU copyright law, however, case law has established that skill and labor (like the U.S. "sweat of the brow" doctrine) are insufficient to confer copyright protection on a database and it is the selection and arrangement of data in the database, not in the creation of the data, that determines whether copyright protection may be available for a database. The European Court of Justice has explained that the "criterion of originality is satisfied when, through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices . . . and thus stamps his 'personal touch.' " This criterion is "not satis-

---

[Section 5.10[1]]

[1]Commission Directive 7934/95 of March 11, 1996, on the Legal Protection of Databases, 1996 O.J. (L077) 20, at chapter III ("Database Directive"), Art. 7(1). This provision grew out of a 1992 European Economic Community initiative intended as a rejection of the analysis employed in *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991). *See* Jack E. Brown, "Proposed International protection of Electronic Databases," The Computer Law., Jan. 1997, at 17, 18. A copy of the Directive may be obtained at http://guagua.echo.lu.legal/en/ipr/database.

[2]Database Directive Art. 1(2); Preamble ¶ 17. Elements of a database, however, need not be "physically stored in an organized manner." Jack E. Brown, "Proposed International protection of Electronic Databases," The Computer Law., Jan. 1997, at 21. Excluded from the definition of a database are recordings or audiovisual, cinematographic, literary or musical works. Jack E. Brown, "Proposed International protection of Electronic Databases," The Computer Law., Jan. 1997, at 17.

[3]The EU Copyright Directive is separately addressed in chapter 4. *See supra* § 4.20.

fied when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom."[4]

The Database Directive also does not extend protection to computer programs used in the making or operation of a database, however, which is the subject of a separate EU directive.[5]

Despite its potentially broad coverage, court opinions to date have construed the scope of the Database Directive more narrowly.[6]

The legal protection conferred by the Database Directive is not applicable to a database which is neither eligible for copyright nor *sui generis* protection. Even where a database is entitled to sui generis protection, the Directive establishes mandatory rights for lawful users of a database (which are akin to fair use rights).[7] These rights can be limited by contract, however, if permitted under the applicable national law.[8]

5.10[2] Copyright Protection for Databases

The Directive was intended in part to harmonize copyright protection for databases within the European Union. The EU Database Directive compels protection of databases under the copyright laws of member states which "by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation . . . ."[1] No other criteria—beyond an author's selection or arrangement—may be applied by EU member countries in granting copyright protection to databases.[2] The protection afforded by the Directive, however, does not extend to the contents of

---

[4]*See* Football Dataco Ltd. v. Yahoo UK Ltd., Case C-604/10 (European Court of Justice 2012).

[5]*See* Database Directive Arts. 1, 2.

[6]See British Horseracing Board Ltd. v. William Hill Organization Ltd., Case C-203/02 (European Court of Justice 2004); Fixtures Mktg, Ltd. v. Oy Veikkaus Ab, Case C-46/02 (European Court of Justice 2004).

[7]*See* Database Directive Arts. 6(1), 8, 15.

[8]*See* Ryanair Ltd v. PR Aviation BV, Case C-30/14 (European Court of Justice 2015).

[Section 5.10[2]]

[1]Database Directive Art. 3(1).

[2]*See* Database Directive Art. 3(1); Football Dataco Ltd. v. Yahoo UK Ltd., Case C-604/10 (European Court of Justice 2012).

protected databases and must be provided "without prejudice to any rights subsisting in those contents . . . ."[3]

The Directive recognizes an author's exclusive rights to reproduction, translation, adaptation, arrangement and "any other alteration," public distribution (subject to first sale within the community) and "communication, display or performance to the public," as well as reproduction, distribution, communication, display or performance to the public as a result of translation, adaptation, arrangement or other alteration.[4] While there is no express fair use provision, the Directive allows member states, at their option, to allow for exceptions traditionally recognized under national law or use "for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved."[5] Member states also may allow for exceptions "for the purposes of public security" or "an administrative or judicial procedure."[6] These exceptions are narrower than the U.S. fair use defense.[7]

5.10[3] *Sui Generis* Protection

5.10[3][A] In General

In addition to copyright protection, the EU Database Directive compels member states to provide *sui generis* protection for at least fifteen years from the date of completion of the database[1] to the "maker of a database"[2] who can show "a substantial investment in either the obtaining,

---

[3]Database Directive Art. 3(2).

[4]*See* Database Directive Art. 5.

[5]*See* Database Directive Art. 6.

[6]*See* Database Directive Art. 6(2)(c).

[7]*See supra* § 4.10.

[Section 5.10[3][A]]

[1]*See* Database Directive Art. 10(1).

[2]The term "maker of a database" is not defined, but presumably is not necessarily the same entity as the author in whom copyright protection under the Directive vests. Although maker is not defined, the making of a database is said to require "the investment of considerable human, technical and financial resources . . ." *See* Database Directive Art. 10(1), Preamble ¶ 7. By extension, a maker would be a person or entity that invests such resources. According to one commentator, the term could be broad enough to include companies that provide, but do not themselves compile, data. *See* David Mirchin, "EU Database Directive Has Global

verification or presentation of the contents" to "prevent extraction[3] and/or re-utilization[4] of the whole or of a substantial part of the contents of that database."[5] Whether a substantial investment has been made, or a substantial part . . . extracted or re-utilized, may be evaluated qualitatively and/or quantitatively.[6] The *sui generis* database rights created by the Directive may be transferred, assigned or granted by license.[7] These rights exist independently of any copyright protection which may be available for the database or its contents.[8]

The Directive contains a limited right akin to fair use under U.S. law. Lawful users must be allowed to extract and/or re-utilize insubstantial parts of the contents of a database (judged qualitatively and/or quantitatively).[9] This right is tempered, however, by the requirement that member states prohibit "[t]he repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database."[10] The right to insubstantial extraction or re-utilization, while perhaps more limited, may be easier to apply than fair use under U.S. law, which is determined by a balancing test that focuses on other factors beyond merely the amount and nature of the portion copied.[11]

Member states are further permitted to allow "extraction

Ramifications", Nat. L.J., June 9, 1997.

[3]*Extraction* is defined as "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form." Database Directive Art. 7(2)(a).

[4]*Re-utilization* means "any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission." Database Directive Art. 7(2)(b). First sale within the community, however, exhausts the right to control resale within the EU. Database Directive Art. 7(2)(a).

[5]*See* Database Directive Art. 7(1).

[6]*See* Database Directive Art. 7(2)(a). The term substantial, however, is not defined.

[7]*See* Database Directive Art. 7(3).

[8]*See* Database Directive Art. 7(4).

[9]Database Directive Art. 8.

[10]Database Directive Art. 7(5).

[11]*See supra* § 4.10.

for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved."[12] Exceptions also are recognized for extraction or re-utilization "for the purposes of public security or an administrative or judicial procedure."[13]

5.10[3][B] Territorial Scope of Protection

Protection is available under the EU Database Directive based on the residency of the database owner, not the country or territory where it is created. Rights under the Directive are granted to makers or rightsholders who are nationals of an EU member state or who have their habitual residence within the European Union.[1] A company or firm formed in accordance with the laws of a member state may benefit from the Directive, but only if (1) its "central administration or principal place of business" is located within the EU or (2) its "registered office" is located within the EU and "its operations . . . [are] genuinely linked on an ongoing basis with the economy of a Member State."[2] The Council also is authorized to extend protection to databases made in third countries by persons or entities not entitled to benefit from the Directive, where reciprocal protections are recognized.[3]

5.10[3][C] Term of Protection

The term of *sui generis* protection, while stated as fifteen years, actually is always longer than fifteen years, and potentially may be extended indefinitely.[1] While a database is protected as of the date of completion, the term of protection only expires fifteen years from the first day of January of the year following the date when the database was

---

[12]Database Directive Art. 9(b).

[13]Database Directive Art. 9(c).

[Section 5.10[3][B]]

[1]Database Directive Art. 11(1).

[2]Database Directive Art. 11(2).

[3]Database Directive Art. 11(3), Preamble 56.

[Section 5.10[3][C]]

[1]The term for copyright protection in a database, however, is not extended by the Directive. *See* Database Directive Art. 2(c).

completed.[2]

The term of protection may be extended by making the database available to the public "in any manner" before the expiration of the initial term. In such case, protection shall be extended to fifteen years from the first day of January of the year following the date when the database was first made available to the public.[3] A database made available to the public just prior to the expiration of its initial term therefore could enjoy potentially up to almost thirty-one years of protection (depending on when during the year preceding the commencement of the first fifteen-year term the database was completed).

As a practical matter, protection for a database could be extended indefinitely. If a substantial change is made to the contents of a database, including changes that result "from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment," then the database would be entitled to a new term of protection.[4] The substantiality of any changes or investments may be evaluated qualitatively or quantitatively.[5] Given the extent of revisions required to keep most commercial databases current, it seems likely that owners could extend the term of protection indefinitely, and then still be entitled to over fifteen years of protection after the database is retired from use and no longer updated.

Limited retroactive protection also may exist for certain databases. Specifically, protection must be recognized for any database completed after December 31, 1982, that otherwise complied with the requirements for protection under the Directive on January 1, 1998.[6] Retroactive protection, however, must be granted "without prejudice to any acts concluded and rights acquired" prior to January 1, 1998.[7]

---

[2] *See* Database Directive Art. 10(1).

[3] *See* Database Directive Art. 10(2).

[4] *See* Database Directive Art. 10(3).

[5] Database Directive Art. 10(3).

[6] *See* Database Directive Art. 14(3). The initial term of protection would expire fifteen years from the first of January in the year following the date on which the database was completed. *See* Database Directive Art. 14(5).

[7] *See* Database Directive Art. 14(4).

5.11 Sample Injunction Order

5.11[1] Overview

The following is a form created from the actual order for preliminary and permanent injunctive relief entered by the court in *Craigslist, Inc. v. Naturemarket, Inc.*,[1] where the court granted a default judgment to Craigslist on claims for copyright infringement (based on exceeding the scope of the license for Craigslist's website, set forth in its TOU), DMCA violations (for circumvention of CAPTCHA and other security measures), the Computer Fraud and Abuse Act (for exceeding authorized access as defined by Craigslist's TOU for purposes of employing, implementing and updating software to allow for automated postings on Craigslist), California Penal Code § 502 (for knowingly accessing a computer without permission and causing damage), trademark infringement (in connection with its use of the Craigslist mark in sponsored links),[2] common law trademark infringement (based on use of the mark in advertising defendants' services and auto posting software), breach of contract (the TOU agreement), inducing breach of contract and intentional interference with contractual relations, and fraud. In that case, the defendants sold software products that allowed users to automatically post material to Craigslist's site, in violation of its TOU, and harvest email addresses from the site. Because of the number of claims on which judgment was entered, the order may provide a useful form. Like any form, it must be tailored to the specific facts and claims at issue in a given case.

5.11[2] FORM

Upon consideration of plaintiff's motion for injunctive relief and defendants' opposition, the court hereby orders that defendants __, their employees, representatives, agents and all persons or entities acting in concert with them, are preliminarily and permanently enjoined from:

(a) manufacturing, developing, creating, adapting, modifying, exchanging, offering, distributing, selling, providing,

---

[Section 5.11[1]]

[1]*Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039 (N.D. Cal. 2010).

[2]*See generally infra* § 9.11 (analyzing the law of sponsored links).

importing, trafficking in, or using any automated device or computer program (including but not limited to, any technology, product, service, device, component, or part thereof) that enables postings on __ (the "Website") without each posting being entered manually;

(b) manufacturing, developing, creating, adapting, modifying, exchanging, offering, distributing, selling, providing, importing, making available, trafficking in, or using content that uses automated means (including, but not limited to, spiders, robots, crawlers, data mining tools, and data scraping tools) to download or otherwise obtain data from the Website;

(c) copying, distributing, displaying, creating derivative works or otherwise using protected elements of plaintiff's copyrighted website (located at www._), including but not limited to, the website's post to classifieds, account registration and account log in expressions and compilations, and from inducing, encouraging, causing or materially contributing to any other person or entity doing the same;

(d) circumventing technological measures that control access to plaintiff's copyrighted website and/or portions thereof (including, but not limited to, CAPTCHAs and RECAPTCHAs), and from inducing, encouraging, causing or materially contributing to any other person or entity doing the same;

(e) manufacturing, developing, creating, adapting, modifying, exchanging, offering, selling, distributing, providing, importing, trafficking in, or using technology, products, services, devices, components, or parts thereof, that are primarily designed or produced for the purpose of circumventing technological measures and/or protection afforded by technological measures that control access to plaintiff's copyrighted website and/or portions thereof, and from inducing, encouraging, causing or materially contributing to any other person or entity doing the same;

(f) accessing or attempting to access plaintiff's computers, computer systems, computer network, computer programs, and data, without authorization or in excess of authorized access, including, but not limited to, creating accounts or posting content on the Website, and from inducing, encouraging, causing, materially contributing to, aiding or abetting any other person or entity to do the same;

(g) manufacturing developing, creating, adapting, modifying, exchanging, offering, selling, distributing, providing,

importing, trafficking in, purchasing, acquiring, transferring, marketing or using any program, device, or service designed to provide an automated means of accessing the Website, automated means of creating accounts on the Website or with plaintiff, or automated means of posting ads or other content on the Website, including, but not limited to, any program, device, or service that is, in whole or in part, designed to circumvent security measures on the Website;

(h) repeatedly posting the same or similar content on the Website, posting the same item or service in more than one category on the Website, posting the same item or service in more than one geographic area on the Website, and from inducing, encouraging, causing, assisting, aiding, abetting or contributing to any other person or entity doing the same;

(i) posting ads on behalf of others, causing ads to be posted on behalf of others, and accessing the Website to facilitate posting ads on behalf of others;

(j) using, offering, selling or otherwise providing a third-party agent, service, or intermediary to post content to the Website;

(k) misusing or abusing plaintiff, the Website and plaintiff's services in any way, including, but not limited to, violating plaintiff's TOU;

(l) accessing or using the Website for any commercial purpose whatsoever, and;

(m) using the __ mark and any confusingly similar designation in Internet advertisements and otherwise in commerce in any manner likely to confuse consumers as to their association, affiliation, endorsement or sponsorship with or by the plaintiff.

IT IS SO ORDERED

_____

JUDGE

5.12 Anti-Scraping Measures Pursuant to the Cybersecurity Information Sharing Act

The Cybersecurity Information Sharing Act (CISA)[1] permits companies, including database owners, to take

---

[Section 5.12]

[1]6 U.S.C.A. §§ 1501 to 1510.

certain measures to protect the security of their systems. It also limits a database owner's ability to treat as a cybersecurity threat a Terms of Use violation.

The Act permits companies to take defensive measures to protect their information systems.[2] However, the Act narrowly circumscribes what constitutes a *defensive measure*. A *defensive measure* is defined narrowly as one that addresses the purpose of the statute.[3] The statute also expressly excludes the possibility of relying solely on Terms of Use or other consumer license agreements as a basis for taking a defensive measure against a cybersecurity threat.[4] Thus, while CISA empowers database owners to take added measures to protect the security of their information systems, it also limits their ability to treat contractual violations as cybersecurity threats under the Act.

CISA is analyzed in section 27.04[1.5] of chapter 27.

5.13 Checklist of Potential Ways to Protect Database Content

In General

- Database owners should restrict access and use by contract
- Database owners should employ technological means (including security, access controls and copy protection mechanisms) to block access to material
- Database owners should organize their databases and materials to maximize potential protection under copyright, trademark, trade secret and patent laws
- Database owners should set no scraping tags pursuant to the Robots Exclusion Standard and consider taking other technical measures to restrict scraping

Copyright

- Is the database, as a compilation, entitled to protection based on the selection, arrangement of organization of the compilation?
- Are the individual components of a database independently protectable (such as photos, articles, music and videos) or merely unprotectable data (or

[2] 6 U.S.C.A. § 1503(b)(1); *infra* § 27.04[1.5].

[3] *See* 6 U.S.C.A. § 1503(b)(2); *infra* § 27.04[1.5].

[4] 6 U.S.C.A. § 1501(5)(B); *infra* § 27.04[1.5].

material otherwise in the public domain such as court opinions)?
    - If the "contributions" to the collective work are separately protectable, who owns the copyrights to these works?
    - Does the database owner have rights to the underlying components of the database (either through ownership or a license) or is there a potential *Tasini* problem?[1]
    - Is an implied license defense available?
- Does the extent of copying rise to the level of substantial similarity or virtual identicality?
- Does the copying qualify as fair use intermediate copying?

Contract

- Is there privity of contract between the database owner and the party against whom the agreement is sought to be enforced?
    - If not, can a claim be asserted for tortious interference with contract or interference with prospective economic advantage, based on the third party providing the means for its users to breach their contracts (or could the database owner allege that it is an intended third party beneficiary of the contract)?[2]
- Are the terms presented in a manner in which they are likely to be deemed enforceable?[3]
    - Agreements presented as click-through contracts are more likely to be enforced than terms that are merely posted on a site
    - Is the agreement susceptible to being challenged as unconscionable?[4]
- May the agreement be characterized as a license or mere contract?

[Section 5.13]

[1]*See supra* § 5.01.

[2]*See supra* § 5.03[5].

[3]*See infra* § 21.03; *see generally infra* chapters 21, 22 (analyzing Terms of Use and enforceable unilateral contracts). Some database companies obtain signed, written contracts, or negotiate the terms of an agreement, which eliminates the formation issues addressed here.

[4]*See infra* §§ 21.05 (unconscionability and checklist), 22.05[2][M] (arbitration and class action provisions and unconscionability), 22.05[4]

- Is the compilation protectable under copyright law?
- Are licensees given access to software or other protectable material in addition to factual data or other material in the public domain?
- Is the agreement susceptible to being challenged under the copyright misuse doctrine?[5]

- Do the terms of the contract adequately protect the database owner? Common terms include prohibitions on:
  - Commercial use of the database or website, including duplication and downloading of content;
  - The use of bots, scripts, executable code, intelligent agent software, spiders, crawlers or other automated means of accessing the site or extracting data;
  - Accessing the site more than a set number of times in a given time period;
  - Taking any action that imposes an unreasonable burden or disproportionately uses system resources;[6]
  - Using the site in any manner not expressly licensed; and
  - Use after termination of the agreement
- Does the agreement include carve-outs that could allow certain uses, either because what is being licensed is narrowly defined or particular uses or data (such as material in the public domain) are excluded?[7]

Common Law Misappropriation

- Does the claim allege an extra element beyond mere copying?
- Was copying undertaken to provide information sooner than when users might otherwise receive it (i.e., "hot news")?[8]

Trespass

- Was access unauthorized based on contractual terms or notice?

(draftsmanship).

[5] *See supra* § 5.03[1].

[6] *See supra* § 5.03[2].

[7] *See supra* § 5.03[3].

[8] *See supra* § 5.04.

- May a claim for trespass to chattels be brought for trespass to an intangible under applicable statute law?
- If so, what level of damage can be shown to server capacity or system resources?
  - Injury to a business is not recoverable; the damage must be to the chattel[9]

Conversion

- Was data destroyed or deleted, or were intangible assets taken, or was data merely copied?

Computer Fraud and Abuse Act

- Was access unauthorized (or was authorized access exceeded) based on contractual terms or notice?
  - If authorization was given, has it been revoked?
- Can $5,000 in damages be shown?[10]

DMCA

- Did access involve circumvention of access controls?
- Was copyright management information (CMI) deleted or false CMI added?[11]

BOTS Act

- Did someone circumvent a security measure, access control system, or other technological control or measure that is used by a ticket issuer to enforce posted event ticket purchasing limits or to maintain the integrity of posted online ticket purchasing order rules?

Lanham Act

- Does the use of information from the database include use of the database owner's marks?[12]
  - Could the use be deemed a nominative fair use (use not in a trademark sense)?
  - Does the use involve intermediate copying?
  - Does the use involve passing off goods or services as belonging to the database owner or falsely suggesting sponsorship, affiliation or endorsement by the owner?
  - Is the use likely to cause confusion or dilution?

---

[9] *See supra* § 5.05.

[10] *See supra* § 5.06.

[11] *See supra* § 5.07.

[12] *See supra* § 5.08.

Trade Secret

- Was confidential information entitled to protection as a trade secret misappropriated by someone under a duty to keep it confidential?[13]

Cybersecurity Information Sharing Act

- Is the database owner protecting its information systems pursuant to the Act?[14]

Preemption Considerations

- Are potential claims against third parties preempted by the Good Samaritan Exemption to the Communications Decency Act, 47 U.S.C.A. § 230(c)?[15]
- Are potential claims preempted by the Copyright Act,[16] the Lanham Act,[17] section 7 of the Uniform Trade Secrets Act (where enacted as state law)[18] or the Patent Act?[19]

5.14 Checklist for Ethical Scraping Practices

The following is a checklist of measures to undertake to mitigate the risk of liability under U.S. law for scraping third party content without permission:[1]

- Don't access a site whose TOU or EULA prohibit scraping or non-commercial use of the site;[2]
- Don't scrape any site whose owner or operator has notified you that you are not permitted to access the site

---

[13]*See supra* § 5.09.

[14]*See supra* § 5.12.

[15]*See infra* § 37.05.

[16]*See supra* § 5.04.

[17]*See supra* § 5.08.

[18]*See supra* § 5.09; *infra* § 10.17.

[19]*See supra* § 5.04[3].

[Section 5.14]

[1]This list reflects general "best practices" but is neither a comprehensive list for avoiding exposure nor a statement of legal principles that if violated necessarily would result in liability. As underscored throughout this chapter, what is lawful in the area of database protection and screen scraping depends on the nature of the database, the type of information copied or used by a third party, how it was accessed, and what is being done with it. Businesses engaged in screen scraping may need to make many nuanced decisions to structure their affairs to avoid liability.

[2]*See supra* § 5.03.

or to scrape content or that your access rights have been limited or revoked;

- Don't use bots to encourage sales or votes without disclosing the use of bots, to the extent a party is bound to comply with California's bot disclosure law, which requires a disclosure that is "clear, conspicuous, and reasonably designed to inform persons with whom the bot communicates or interacts that it is a bot."[3]
- Scraped content, where possible, should be used for internal analysis only;
- Original and creative images or text (as opposed to facts), which may be entitled to copyright protection, should not be used commercially or copied to websites or other publicly available documents or locations without permission (unless a fair use);[4]
- Scraping should be undertaken during off hours and in a manner to ensure that there is no substantial impairment to the target site's server capacity;[5]
- Avoid using scraped data to "scoop" competitors with time sensitive information;[6]
- Do not circumvent technical measures or access controls to scrape content[8] and do not scrape material from private locations (or non-public locations where access is restricted) or seek to gain access to a proprietary location to scrape content under false pretenses;
- Don't circumvent a security measure, access control system, or other technological control or measure that is used by a ticket issuer to enforce posted event ticket purchasing limits or to maintain the integrity of a posted online ticket purchasing order rule;[8] and
- Honor the Robot Exclusion Standard and similar protocols or tags that alert third parties not to access a site using bots or intelligent agents.[9]

---

[3]Cal. Bus. & Prof. Code § 17941(b); *infra* § 5.16.

[4]*See supra* § 5.02. If copyrighted material is published, copyright management information (CMI) and logos or other trademark-protected material generally should not be removed. *See supra* §§ 5.07[2], 5.08.

[5]*See supra* § 5.05[1].

[6]*See supra* § 5.04[1].

[8]*See supra* § 5.07[1].

[8]*See supra* § 5.07[3].

[9]*See supra* § 5.05[1].

5.15 Managing By Contract the IP Liability Risks of Artificial Intelligence

Artificial intelligence raises a host of policy questions. Even defining AI presents challenges because bots and AI agents exist on a continuum of autonomy. While there is no fine line between them, AI agents are characterized by one or more of the following: relatively high independence and control over their own actions, the capacity to interact with other agents or users, the ability to proactively initiate goal-oriented behavior, the ability to react and adapt to their environment, the ability to navigate physical or virtual space, and the degree to which they are capable of acting as a representative or intermediary for another agent or person. Independence, interactivity, and proactivity may be the most important factors.[1]

From an IP perspective, when AI is deployed, liability likely would fall on the person or entity that empowered the agent, much as liability may be imposed on a principal for the conduct of an agent. If software agents using AI scrape particular data, it would still likely be the responsibility of the entity that programmed the agent, much in the same way that a business is responsible for any misconduct by an employee acting within the scope of employment.

In general, use of AI agents could expose corporations to liability because knowledge obtained by corporate agents acting within the scope of employment and for the benefit of the corporation may be imputed to the corporation,[2] and corporations are generally responsible for the collective knowledge of their agents.[3] While questions remain whether *knowledge* could be imputed to an algorithm for purposes of agency law, the notion that a person or entity who deploys

---

[Section 5.15]

[1] *See* Samir Chopra & Laurence F. White, A LEGAL THEORY FOR AUTONOMOUS ARTIFICIAL AGENTS 9-10 (2011).

[2] *See, e.g.*, *Helton v. AT&T Inc.*, 709 F.3d 343, 356 (4th Cir. 2013); *Primal Eagle Grp. v. Steel Dynamics, Inc.*, 614 F.3d 375, 378-79 (7th Cir. 2010); *Universal Pictures Co. v. Harold Lloyd Corp.*, 162 F.2d 354, 371 (9th Cir. 1947); *United States ex rel. Miller v. Bill Harbert Int'l Constr., Inc.*, 608 F.3d 871, 901 (D.C. Cir. 2010).

[3] *See, e.g.*, *United States v. Bank of New England*, 821 F.2d 844, 856 (1st Cir.), *cert denied*, 484 U.S. 943 (1987); *Gutter v. E.I. DuPont Nemours*, 124 F. Supp. 2d 1291, 1309 (S.D. Fla. 2000); *see also* 3 WILLIAM MEADE FLETCHER, CYCLOPEDIA OF THE LAW OF CORPORATIONS § 790 ("[T]he cumulative knowledge of several agents can be imputed to the corporation.").

an algorithm should be responsible for the subsequent acts and omissions initiated by the algorithm appears sound.

Imposing liability on the person or entity that deployed an algorithm to collect data or information is also consistent with basic concepts of general and proximate causation.

Absent a statutory or contractual provision to the contrary, a business that deploys an algorithm to scrape data and information from third party sites may be responsible for the acts and omissions occasioned by the algorithm in a dispute with an innocent third party.

Many potential IP disputes involving AI may be anticipated in advance and resolved by contract or license.[4] For example, if one party provides tools to deploy an intelligent avatar using the attributes of a third party, permission generally would be required to use those attributes (unless the use was fair, licensed, or otherwise permissible).[5] Likewise, it would be prudent for the parties to determine in advance what their respective rights will be with respect to the creative output of the intelligent agent.[6] The same is true for developers of intelligent software. Publishers may elect to provide a tool that creates intellectual property owned by a customer or the publisher, or both, with exclusive or non-exclusive license rights carved out. Absent a contract, however, liability potentially could be premised on a theory

---

[4] *See infra* §§ 16.01 to 16.04 (analyzing licenses and contracts).

[5] Rights of publicity are analyzed in chapter 12.

[6] At common law, computer programs are generally considered instrumentalities rather than agents. RESTATEMENT (THIRD) OF AGENCY § 1.04 cmt. e (AM. LAW INST. 2006). But this understanding is based on "present" capabilities, *id.*, and as AI agents grow in sophistication, courts may look to agency theory for guidance in assessing liability. *See generally Samir Chopra & Laurence F. White, A Legal Theory for Autonomous Artificial Agents* 9-10 (2011) (advancing normative and doctrinal grounds for applying agency theory to AI agents). In *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1568, 54 Cal.Rptr.2d 468, 474 (4th Dist. 1996), for example, an intermediate appellate court in California characterized Thrifty-Tel's "computerized network as an agent or legal equivalent" such that Bezenek's misrepresentations to the network could be imputed to Thrifty-Tel. More extreme would be directly granting AI agents a form of legal personhood, as with corporations. The European Parliament has adopted a non-binding resolution calling on the European Commission to explore this very possibility. *See* European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), EUR. PARL. DOC. P8__TA(2017)0051, ¶ 59(f), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN.

of negligent training or supervision, especially for AI agents trained using supervised or reinforcement learning methods.[7]

There are open questions about the extent to which AI can generate intellectual property. Copyright law, for example, only extends protection to original and creative expression.[8] Whether original expression created through artificial intelligence is the work product of the agent or the human who created the agent remains to be fully fleshed out.[9] To the extent a work is created by artificial means and not a person, however, it may not be registered with the U.S. Copyright Office.[10] Moreover, only humans have standing to sue for copyright infringement.[11]

Liability for agents empowered by AI may be varied by contract or subject to indemnification obligations or insurance, but the party that deployed an agent in most cases will be liable for the actions it directed, preprogrammed, or enabled through AI. With respect to screen scraping by bots, whether intelligent agents or agents using artificial intelligence, the liability regime established by contract, common law rules such as trespass and statutes such as the Computer Fraud and Abuse Act (as addressed throughout this chapter) will largely be the same.

The underlying algorithms used for machine learning and

---

[7]The doctrine of negligent supervision holds employers liable for negligence in the hiring, training, and supervision of their employees. *See* RESTATEMENT (THIRD) OF AGENCY § 7.05(1).

[8]*See supra* § 5.02.

[9]For example, In *Design Data Corp. v. Unigate Enterprise, Inc.*, 847 F.3d 1169 (9th Cir. 2017), the Ninth Circuit raised without deciding the question of whether the owner of a copyrighted computer aided design (CAD) program could claim protection in the program's output, and not merely the program itself, in circumstances where "the program 'does the lion's share of the work' in creating the output and the user's role is so 'marginal' that the output reflects the program's content." *Id.* at 1173, *citing* 4 Nimmer on Copyright § 13.03[F] (quoting *Torah Soft Ltd. v. Drosnin*, 136 F. Supp. 2d 276, 283 (S.D.N.Y. 2001)). Although the appellate panel seemed skeptical that the output of a program could be protectable, it nonetheless affirmed summary judgment for the defendant on this issue because the plaintiff had not introduced evidence to meet the plaintiff's proposed standard, regardless of whether it was applicable.

[10]*See* U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 313.2 (3d ed. 2017).

[11]*See, e.g.*, *Naruto v. Slater*, 888 F.3d 418, 426 (9th Cir. 2018) (holding, in the Monkey Selfie case, that "animals other than humans . . . lack statutory standing to sue under the Copyright Act.").

automated decision-making are potentially patentable, if novel and nonobvious,[12] or entitled to protection as trade secrets.[13] They may also be entitled to copyright protection.[14]

Using artificial intelligence or automated decision making also potentially implicates privacy laws, as addressed in section 26.03A in chapter 26. Disclosure requirements when bots are used to encourage sales or political votes are analyzed in section 5.16.

5.16 Laws Requiring Disclosure of the Use of Bots

While the use of bots and AI generally need not be disclosed, in some contexts the failure to disclose use of scripts or AI could be deemed actionable. California's Bot Disclosure Law,[1] for example, which took effect in 2019, makes actionable the undisclosed use of bots to encourage sales or political votes. Specifically, it makes it unlawful "for any person[2] to use a bot to communicate or interact with another person in California online,[3] with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election."[4] For purposes of the statute, a bot is defined as "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person."[5]

A person using a bot may avoid liability under the statute

---

[12]Patent protection is analyzed in chapter 8.

[13]Trade secret protection is analyzed in chapter 10.

[14]*See supra* § 4.07 (copyright protection for computer software).

[Section 5.16]

[1]Cal. Bus. & Prof. Code §§ 17940 *et seq*.

[2]A *person* is defined as "a natural person, corporation, limited liability company, partnership, joint venture, association, estate, trust, government, governmental subdivision or agency, or other legal entity or any combination thereof." Cal. Bus. & Prof. Code § 17940(d).

[3]*Online*, under the statute, means "appearing on any public-facing Internet Web site, Web application, or digital application, including a social network or publication." Cal. Bus. & Prof. Code § 17940(b).

[4]Cal. Bus. & Prof. Code § 17941(a).

[5]Cal. Bus. & Prof. Code § 17940(a).

simply by disclosing the use of the bot.[6] To be effective, the disclosure must be "clear, conspicuous, and reasonably designed to inform persons with whom the bot communicates or interacts that it is a bot."[7]

While the duties and obligations imposed by California's bot disclosure law are intended to be cumulative with any other duties or obligations imposed by any other law,[8] they are not intended to apply to platforms or other types of service providers.[9]

5.17 Laws Protecting Data Integrity

With the increased use of AI and machine learning, data integrity has become a greater concern. Machine learning is only as good as the test sets used to train an algorithm how to respond. If data is incomplete or inaccurate, algorithms will provide flawed analysis and outcomes.

There is no single law governing data integrity. Database owners have an interest in data integrity to ensure that the products, services or data they provide are accurate and reliable. Their business partners, in turn, may rely on the accuracy and integrity of data provided for machine learning or other purposes. Consumers, in turn, may have an interest in ensuring that data about themselves is accurate (or conversely an interest in deleting or modifying accurate data which impairs their ability to obtain credit or employment or has other consequences in the modern world, but which could undermine the integrity of the data).

When data integrity is compromised, it is usually due to mistakes, not sabotage. In such circumstances, database owners and licensees may have contractual remedies, depending on what their contracts provide. Database owners also may be able to avail themselves of the various remedies

---

[6] *See* Cal. Bus. & Prof. Code § 17941(a).

[7] Cal. Bus. & Prof. Code § 17941(b).

[8] *See* Cal. Bus. & Prof. Code § 17942(a).

[9] Cal. Bus. & Prof. Code § 17942(c) (providing that the bot disclosure law shall "not impose a duty on service providers of online platforms, including, but not limited to, Web hosting and Internet service providers."). An *online platform* means "any public-facing Internet Web site, Web application, or digital application, including a social network or publication, that has 10,000,000 or more unique monthly United States visitors or users for a majority of months during the preceding 12 months." *Id.* § 17940(c). Platform liability and immunities and safe harbors are addressed in chapter 49.

outlined in this chapter, including the Computer Fraud and Abuse Act, which potentially provides a remedy (where the other elements of the statute are met) for "any impairment to the integrity or availability of data, a program, a system or information . . . ."[1] On the other hand, some remedies otherwise available to database owners to address screen scraping do not extend to data integrity.[2]

Consumers, by contrast, may not have standing or other grounds to challenge data integrity, except under privacy laws (as detailed in chapter 26). Indeed, suits against a database operator over false information (including instances where a known or unknown third party alters or manipulates data) may be preempted by the Communications Decency Act (or CDA),[3] which immunizes interactive computer ser-

---

[Section 5.17]

[1]*See* 18 U.S.C.A. § 1030(e)(8); *see generally supra* § 5.06 (analyzing the CFAA).

[2]*See, e.g.*, *WhatsApp Inc. v. NSO Group Technologies Ltd.*, 472 F. Supp. 3d 649, 683-86 (N.D. Cal. 2020) (dismissing plaintiffs' trespass claim, with leave to amend, where plaintiffs alleged that defendants impaired the value and quality of WhatsApp's servers by designing a program that concealed malicious code and made it appear that WhatsApp, rather than defendants, sent the code, reasoning that this argument conflated the impairment of the value and quality of WhatsApp's servers with the impairment to "the integrity, quality, and value of WhatsApp's services . . . .") (*citing Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1347, 1358, 1 Cal. Rptr. 3d 32 (2003); *Hiossen, Inc. v. Kim*, No. CV1601579SJOMRWX, 2016 WL 10987365, at *11 (C.D. Cal. Aug. 17, 2016) (holding that a financial injury resulting from trespass to a computer is not an actual harm under *Hamidi*); *Fields v. Wise Media, LLC*, No. C 12-05160 WHA, 2013 WL 5340490, at *4 (N.D. Cal. Sept. 24, 2013) (same)), *aff'd on other grounds,* __ F.4th __, 2021 WL 5174092 (9th Cir. 2021). *But see Microsoft Corp. v. Does 1–18,* No. 13cv139 (LMB/TCB), 2014 WL 1338677, at *10 (E.D. Va. Apr. 2, 2014); *CompuServe Inc. v. Cyber Promotions, Inc.,* 962 F. Supp. 1015, 1023 (S.D. Ohio 1997).

[3]*See, e.g.*, *924 Bel Air Road, LLC v. Zillow Group, Inc.*, Case No. 2:19-CV-01368-ODW (AFMx), 2020 WL 774354, at *2-4 (C.D. Cal. Feb. 18, 2020) (dismissing as preempted by the CDA, without leave to amend, plaintiff's negligence claim in a suit arising from an unknown third party "claiming" the Zillow listing for a $100 Million property and creating a false sales record that caused the property to be removed from the 'elite status of a $100M plus property' list and allegedly shifted market perceptions about the property, over plaintiff's argument that its negligence claim was not premised on the unknown user's publication of false information but on Zillow's own allegedly "inadequate monitoring system" that allowed the user to post false content to the site, as merely another way of saying that Zillow should be held liable for republishing the user's content;

vice providers, including database providers, for claims seeking to hold them liable for content originating with third parties (excluding certain claims pertaining to intellectual property, among others).[4] While the CDA provides immunity for claims based on data or other content originating with third parties, it does not insulate a database provider from direct liability for its own acts or omissions unrelated to republication of third party content.[5] The CDA likewise potentially insulates a database operator from claims arising out of a consumer's effort to have accurate information removed from a database.[6] Such claims may arise where data has always been publicly available but previously was not widely accessible (such as high school yearbook photos) or where a consumer seeks to remove information that—which accurate—may adversely affect a user.

The need for data integrity for accurate machine learning is in tension with data privacy laws, which allow in some instances individuals to remove information—particularly the European Union's right to be forgotten. Opt-out rights under E.U. and California and other U.S. state laws protect individual privacy but also may threaten the completeness or accuracy of some data sets.[7] For example, under E.U. law, Article 22(1) of the GDPR, affords individuals, subject to certain exceptions, "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or

---

"Ultimately, Bel Air's allegations boil down to a charge that Zillow must prevent users from falsely claiming a Residence Page or posting false content. Yet, reviewing each user's activity and postings to ensure their accuracy is precisely the kind of activity for which Congress intended section 230 to provide immunity."), *appeal dismissed,* No. 20-55283, 2020 WL 8910588 (9th Cir. Oct. 23, 2020).

[4]*See* 47 U.S.C.A. § 230(c); *see generally infra* § 37.05.

[5]*See* 47 U.S.C.A. § 230(c); *see generally infra* § 37.05.

[6]*See, e.g.*, *Callahan v. Ancestry.com, Inc.*, Case No. 20-cv-08437-LB, 2021 WL 783524, at *5-6 (N.D. Cal. Mar. 1, 2021) (holding Ancestry.com to be an interactive computer service provider of yearbook records, in an opinion holding it entitled to CDA immunity for California right of publicity, intrusion upon seclusion, unjust enrichment and unlawful and unfair business practices claims, arising out of defendant's use of their yearbook photos and related information in its subscription database).

[7]*See generally infra* §§ 26.04 (E.U. law), 26.13A (California law), 26.13C (Virginia law).

similarly significantly affects him or her."[8]In addition to laws and contractual obligations, AI is impacted by data ethics principles promulgated by Google,[9] Facebook,[10] Microsoft,[11] and other AI developer. AI developer ethics and best practices may focus on issues such as transparency (what and how an algorithm is doing, tempered by trade secret, cybersecurity and other proprietary considerations that militate against full transparency), privacy and security (dictated by legal requirements and supplemented in some cases by responsiveness to consumer expectations), fairness (to address or correct for past inequity reflected in data—for example, lending records tainted by redlining and racial bias), and data integrity.

Companies such as Amazon.com also make large datasets available to others to help improve the accuracy of machine learning and AI.[12]

---

[8]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, art. 22(1), 2016 O.J. (L 119) 1, 46; *see also* Stefanie Hänold, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, *in* Robotics, AI and the Future of Law 123, 133-40 (Marcelo Corrales et al. eds., 2018); *see generally infra* § 26.04.

[9]*See* Our Principles—Google AI, https://ai.google/principles/

[10]*See* Facebook's five pillars of Responsible AI (june 22, 2021), *available at* https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/

[11]*See* Responsible AI Principles from Microsoft, https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6

[12]*See Making AI More Accurate, available at* https://www.aboutamazon.com/news/amazon-ai/making-ai-more-accurate (updated Aug. 6, 2019).

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2022

Ian C. Ballon

2022 UPDATES – INCLUDING NEW AND IMPORTANT FEATURES

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator – a 5 volume-set & On Westlaw!

To order call **1-888-728-7677**
or visit **IanBallon.net**

Key Features of E-Commerce & Internet Law

- AI, ML, screen scraping and data portability
- Antitrust in the era of techlash
- The CPRA, Virginia, Colorado and Nevada pricy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- Software copyrightability and fair use after *Google v. Oracle*
- Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- The law of SEO and SEM – and its impact on e-commerce vendors
- Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi,* patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- Enforcing judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Applying the First Sale Doctrine to virtual goods
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- Click fraud
- Copyright and Lanham Act fair use
- Practical tips, checklists and forms that go beyond the typical legal treatise
- Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ AI/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- Addresses both law and best practices
- Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

Volume 1

Volume 2

Volume 3

Volume 4

Volume 5

"Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet."
Jay Monahan
General Counsel, ResearchGate

****

ABOUT THE AUTHOR

****

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.

Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

Mr. Ballon is also the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.lanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@lanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2022

- **Antitrust in the era of techlash** (chapter 34)
- **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurty breach, data privacy, AdTech and TCPA class action suits.**
- **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States,* 141 S. Ct. 1648 (2021)** (ch5)
- **FOSTA-SESTA** and ways to maximize CDA protection (ch 37)
- **IP aspects of the use of #hashtags** in social media (ch 6)
- The **CLOUD Act** (chapter 50)
- **Virginia, Colorado and Nevada privacy laws** (ch 26)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- **Digital economy litigation strategies**
- **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- **Website and mobile accessibility** under the ADA and state laws (chapter 48)
- **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- Updated **Defend Trade Secrets Act** and UTSA case law (chapter 10)
- **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- **AdTech law** (chapter 28, Darren Abernethy)
- **The risks of being bound by the CASE Act's ostensibly *voluntary* jurisdiction over small copyright cases**
- **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Idea protection & misappropriation** (ch 13)
- Revisiting **links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- **eSIGN case law** (chapter 15)