MITCHELL | HAMLINE School of Law

Cybaris®

Volume 12 | Issue 1 Article 1

2021

Data as the New Oil: A Slippery Slope of Trade Secret Implications Greased by the California Consumer Privacy Act

Megan Marie Miller

DATA AS THE NEW OIL: A SLIPPERY SLOPE OF TRADE SECRET IMPLICATIONS GREASED BY THE CALIFORNIA CONSUMER PRIVACY ACT

Megan M. Miller[1]

Table of Contents

[1] Megan is a student at Mitchell Hamline School of Law and has been a practicing Intellectual Property paralegal for over thirteen years. Her biographical information may be found on LinkedIn at https://www.linkedin.com/in/megan-miller-49b8122b/.

The author would like to thank Nadeem W. Schwen for suggesting the topic of this paper, Professor Sharon K. Sandeen for her helpful feedback during the writing process, and the Cybaris team for their refined edits.

Introduction

Following the European model of the General Data Protection Regulation (GDPR), the state of California implemented the California Consumer Privacy Act (CCPA) on January 1, 2020.[2] The CCPA allows any California consumer to demand to see all of the information that a company has saved on them; consumers can also request a full list of all the third parties that their data is shared with, sold to, and for what commercial purpose.[3] This paper reviews the implications of a new law on the disclosure of trade secrets like client lists and algorithms that manipulate consumers' data. Ultimately, the issue comes down to which rights are more important: personal privacy or trade privacy?

When Data Sharing Goes Wrong: Why Privacy Laws Are Necessary

More than 185 million people in the United States and Canada use Facebook® on a daily basis.[4] Facebook monetizes user information through targeted advertising, which generated most of the company's $55.8 billion in revenues in 2018.[5] To encourage users to share information on its platform, Facebook promises users they can control the privacy of their information through Facebook's privacy settings.[6]

Among other things, a 2012 Federal Trade Commission (FTC) order prohibited Facebook from making misrepresentations about the privacy or security of consumers' personal information, and the extent to which it shares personal information, such as names and dates of birth, with third

[2] Cal. Consumer Prot. Act, CAL. CIV. CODE §§ 1798.100-199 (Deering 2020).
[3] *Id.*
[4] Federal Trade Comm'n, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.
[5] *Id.*
[6] *Id.*

parties.[7] The FTC alleged that "Facebook violated the 2012 order by deceiving its users when Facebook shared the data of users' Facebook friends with third-party app developers, even when those friends had set more restrictive privacy settings."[8]

Facebook "launched various services such as 'Privacy Shortcuts' in late 2012 and 'Privacy Checkup' in 2014 that claimed to help users better manage their privacy settings."[9] However, these services "allegedly failed to disclose that even when users chose the most restrictive sharing settings, Facebook could still share user information with the apps of the user's Facebook friends—unless they also went to the 'Apps Settings Page' and opted out of such sharing."[10] The FTC alleged that Facebook did not disclose anywhere on the Privacy Settings page or the 'About' section of the profile page that Facebook could still share information with third-party developers on the Facebook platform about an app users Facebook friends.[11]

Further, "Facebook announced in April 2014 that it would stop allowing third-party developers to collect data about the friends of app users ('affected friend data')."[12] Despite this promise, Facebook "told developers that [the developers] could collect this data until April 2015 if they already had an existing app on the platform."[13] The FTC alleged that Facebook waited "until at least June 2018 to stop sharing user information with third-party apps used by their Facebook friends."[14]

The FTC also alleged that Facebook "misrepresented users' ability to control the use of facial recognition technology with their accounts."[15] According to the complaint, Facebook's

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*

updated data policy from April 2018 "was deceptive to tens of millions of users who have Facebook's facial recognition setting called 'Tag Suggestions' because that setting was turned on by default, and the updated data policy suggested that users would need to opt-in to having facial recognition enabled for their accounts."[16]

In addition to these violations of its 2012 order, the FTC alleged that "Facebook violated the FTC Act's prohibition against deceptive practices when it told users it would collect their phone numbers to enable a security feature [] but did not disclose that it also used those numbers for advertising purposes."[17]

Following a yearlong investigation by the FTC, the Department of Justice filed a complaint on behalf of the FTC alleging that Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences in violation of its 2012 FTC order.[18] "These tactics allowed the company to share users' personal information with third-party apps that were downloaded by the user's Facebook 'friends.'"[19] The FTC alleged "that many users were unaware that Facebook was sharing such information, and therefore did not take the steps needed to opt-out of sharing."[20] The FTC also alleged that Facebook "took inadequate steps to deal with applications that it knew were violating its platform policies."[21]

In 2019, the FTC charged Facebook for violating their 2012 FTC order by "deceiving users about their ability to control the privacy of their personal information."[22] Facebook was ordered to pay a record-breaking $5 billion penalty and submit to new restrictions and a modified corporate

[16] *Id.*
[17] *Id.*
[18] *Id.; see also* Complaint for Civil Penalties, Injunction, and Other Relief, 1-5, 50, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019).
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

structure to "hold the company accountable for the decisions it makes about its users' privacy."[23] "The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide."[24] This penalty is also one of the most substantial penalties "ever assessed by the U.S. government for *any* violation."[25]

As part of Facebook's order-mandated privacy program, which also covers WhatsApp and Instagram, Facebook must conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy.[26] Designated compliance officers at Facebook must generate a quarterly privacy review report, which they must share with the CEO and an independent assessor; they must also share these reports with the FTC upon request.[27] The order also requires Facebook to document incidents themselves and its efforts to address such incidents when data of 500 or more users has been compromised, and deliver this documentation to the FTC and the assessor within 30 days of Facebook's discovery of the incident.[28]

The $5 billion Facebook fine has provided a great example of what not to do in the privacy world and why privacy laws are necessary to protect individual rights. However, Facebook is a for-profit business that has likely spent a significant amount of time and money on creating innovative business methods, and businesses should be entitled to the fruits of their innovations

[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.; see also* Plaintiff's Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief and Memorandum in Support, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019).
[27] *Id.*
[28] *Id.*

that potentially qualify as trade secrets. So how do we balance a company's innovation rights with an individual's privacy rights?

Privacy Law Background

The European Union (EU) implemented the General Data Protection Regulation (GDPR) on May 25, 2018.[29] Though the GDPR was drafted and passed by the EU, it imposes obligations onto organizations anywhere so long as they target or collect data related to people in the EU.[30] The GDPR "will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros."[31]

By implementing the GDPR, "Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and data breaches are a daily occurrence."[32] The GDPR is "large, far-reaching, and fairly light on specifics," which makes GDPR compliance "a daunting prospect, particularly for small and medium-sized enterprises (SMEs)."[33]

The United States has no fully federal law like the GDPR; what currently exists is a patchwork of federal laws and regulations along with some individual state laws.[34] For example, the Health Insurance Portability and Accountability Act (HIPAA) set national standards for protecting the confidentiality, integrity, and availability of electronic protected health

[29] 2016 O.J. (L 119) 1. 2016/679.
[30] *Id.* Article 3(1)
[31] Ben Wolford, *What is GDPR, the EU's new data protection law?*, (Accessed 7 April 2020), available at: https://gdpr.eu/what-is-gdpr/.
[32] *Id.*
[33] *Id.*
[34] Sean Hackbarth, *A Patchwork is Not Acceptable': Making the Case for a National Privacy Law,* U.S. Chamber of Com. – Above the Fold (Jul. 29, 2019, 9:00 A.M.), https://www.uschamber.com/series/above-the-fold/patchwork-not-acceptable-making-the-case-national-privacy-law

information.[35] The Gramm-Leach-Bliley Act requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.[36] The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records.[37] FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.[38] The CAN-SPAM Act sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to opt out of emails, and spells out tough penalties for violations.[39]

At the state level, there is the California Consumer Protection Act (CCPA), which, at the time this paper is being written, just went into effect a few months ago on January 1, 2020.[40] The CCPA is the first state-level privacy law in the United States whih gives the strongest privacy rights to consumers, and is setting the pace for other proposed state privacy legislation.[41] Minnesota is one of the many states endeavoring to enact legislation similar to the CCPA.[42] Proposed by Representative Steve Elkins in March 2020, Minnesota bill HF 3936 models the CCPA.[43] HF 3936 would potentially apply to large Minnesota companies and other companies that intentionally market to Minnesota residents which hold data for over 100,000 consumers or derive over half of their revenue from the sale of personal information and have information about

[35] Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d (1996).
[36] Gramm-Leach Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809, §§ 6821-6827 (1999).
[37] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (1974).
[38] 34 C.F.R Part 99.1 (2012).
[39] CAN-SPAM Act, 16 C.F.R. §316 (2003).
[40] Cal. Consumer Prot. Act, CAL. CIV. CODE §§ 1798.100-199 (Deering 2020).
[41] Gilad Edelman, *California's Privacy Law Goes Into Effect Today. Now What?*, WIRED, Jan 1, 2020, https://www.wired.com/story/ccpa-guide-california-privacy-law-takes-effect/.
[42] H.R. 3936, 91st Leg., Reg. Sess. (Minn. 2020).
[43] *Id.*

at least 25,000 consumers.[44] However, the proposed Minnesota legislation includes additional definitions specific to geolocation data and facial recognition data that the CCPA does not cover.[45]

If each of the fifty states enacts legislation similar, but not uniform, to the CCPA, it will place an unrealistic burden on companies to potentially comply with fifty different versions of privacy laws if a company wants to do business in all fifty states. However, individual state legislation will likely be necessary before the federal government steps in and enacts a law, even though the federal law will likely preempt all of the individual state laws. While certain legislation is more appropriately left to the states instead of the federal government, businesses will be greatly advantaged to only have to comply with a single federal law as opposed to having to comply with fifty individual state laws. Nevertheless, states will be able to set the tone of federal legislation by first creating their own laws, which is what the Founding Fathers wanted—for states to be a laboratory of creating law. Regardless of whether more states enact privacy laws, or the federal government finally does, the CCPA will be influential because it is the most comprehensive privacy law that currently exists in the United States.

The California Consumer Privacy Act (CCPA)

California implemented the California Consumer Privacy Act (CCPA) on January 1, 2020.[46] The Act provides California residents with the right to:

1) Know what personal data is being collected about them;
2) Know whether their personal data is sold or disclosed and to whom;
3) Know the business or commercial purpose for collecting or selling personal information.
4) Opt-out of the sale of personal data;
5) Access their personal data;

[44] *Id.*
[45] *Id.*
[46] Cal. Consumer Prot. Act, CAL. CIV. CODE §§ 1798.100-199 (Deering 2020).

6) Request a business to delete any personal information about a consumer collected from that consumer; and
7) Not be discriminated against for exercising their privacy rights.[47]

The CCPA applies to any business that collects consumers' personal data, with the exception of non-profits and governmental entities.[48] The CCPA defines a "business" as any sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is not considered a nonprofit entity under the California Nonprofit Corporation Law.[49]

Although the CCPA does not define "doing business," a typical definition can be found in the California Revenue and Taxation Code.[50] A company is doing business in California if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California, or if any of the following conditions are satisfied:

1) The business is organized or commercially domiciled in California;
2) Sales[51] of the business in California, including sales by the agents and independent contractors of the business, exceed the lesser of $500,000 or 25% of the business' total sales; [52]
3) Real and tangible personal property of the business in California exceed the lesser of $50,000 or 25% of the business's total real and tangible personal property; or
4) The amount that the business pays for compensation in California exceeds the lesser of $50,000 or 25% of the total compensation paid by the business.[53]

[47] *Id.*
[48] *Id.* at § 1798.140(c).
[49] The California Nonprofit Corporation Law (Division 2 of the Title 1 of the California Corporations Code) provides that nonprofit entities can incorporate as Nonprofit Public Benefit Corporations, Nonprofit Mutual Benefit Corporations, or Nonprofit Religious Corporations. The law further provides that an unincorporated nonprofit association must contain language in its creating document that the association is not allowed to keep the proceeds from business activities and the proceeds must be used for nonprofit purposes.
[50] Cal. Rev. & Tax. Code § 23101 (2012).
[51] As defined in Cal. Rev. & Tax. Code § 25120, subdiv. (e) or (f).
[52] For purposes of Cal. Rev. & Tax. Code § 23101, sales in California are determined using the rules for assigning sales under Cal. Rev. & Tax. Code § 25135, 25136(b) and the regulations thereunder, as modified by regulations under § 25137.
[53] As defined in Cal. Rev. & Tax. Code § 25120.

For the conditions above, the sales, property, and payroll of the taxpayer include the business' pro rata or distributive share of pass-through entities.[54] "Pass-through entities" means partnerships, LLCs treated as partnerships, or S corporations.[55]

Thus, companies that meet the requirements above as "doing business in California" are subject to the CCPA if one or more of the following are true:

1) The business has gross annual revenues in excess of $25 million; or
2) The business buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices; or
3) The business derives fifty percent or more of annual revenues from selling consumers' personal information.[56]

The CCPA also applies to businesses that "control," are "controlled by," or have "common branding" with a business that satisfies one or more of the above-identified criteria.[57] Businesses that handle the personal information of more than four million consumers will also have additional obligations.[58]

"There are various partial exemptions available for certain types of information collected by entities that are also subject to federal privacy laws."[59] The most important and potentially relevant exemptions apply to certain information processed, or to businesses covered, pursuant to the protections of certain federal regulations.[60] "For example, HIPAA-covered entities (and business associates) are not exempt from the CCPA, but protected health information collected by a covered entity or business associate governed by the privacy, security and breach notification

[54] Cal. Rev. & Tax. Code § 23101.
[55] *Id.*
[56] Cal. Consumer Prot. Act, CAL. CIV. CODE §§ 1798.100-199 (2020).
[57] Cal. Consumer Prot. Act, CAL. CIV. CODE §§ 1798.100-199 (2020).
[58] Cal. Consumer Prot. Act, CAL. CIV. CODE §§ 1798.100-199 (2020).
[59] Theodore Augustinos and Laura Ferguson, *CCPA Guide: Are You Covered by the CCPA*, JD SUPRA, (January 15, 2019), available at: https://www.jdsupra.com/legalnews/ccpa-guide-are-you-covered-by-the-ccpa-38771/.
[60] *Id.*

rules promulgated pursuant to HIPAA is exempt."[61] However, "not all information collected by HIPAA-covered entities and business associates is 'governed by' these rules."[62] For example, IP addresses "collected by a HIPAA covered entity appear to be subject to the requirements and protections of the CCPA, even though protected health information collected by the same entity would be exempt."[63]

Similarly, nonpublic personal information processed by a financial institution subject to the privacy, security and breach notification rules promulgated under the Gramm-Leach-Bliley Act would be exempt, but the financial institution would be required to comply with the CCPA with respect to other information (such as information collected when tracking website visitors or providing targeted online advertisements) collected by the financial institution.[64] In addition, this exemption does not apply to the consumer's right to sue for statutory damages as a result of data breach.[65]

As far as this paper is concerned, the most relevant portions of the CCPA are the disclosure requirements for which companies doing business in California must now comply. Upon the request of a consumer, companies doing business in California must disclose the following:

> 1) The categories of personal information it has collected about that consumer;
> 2) The categories of sources from which the personal information is collected;
> 3) The business or commercial purpose for collecting or selling personal information;
> 4) The categories of third parties with whom the business shares personal information; and
> 5) The specific pieces of personal information it has collected about that consumer.[66]

[61] *Id. citing* Cal. Consumer Prot. Act, CAL. CIV. CODE § 1798.145 (c)(1)(A).
[62] *Id.*
[63] *Id.*
[64] *Id. citing* Cal. Consumer Prot. Act, CAL. CIV. CODE § 1798.145(e).
[65] *Id. citing* Cal. Consumer Prot. Act, CAL. CIV. CODE § 1798.145(f).
[66] Cal. Consumer Prot. Act, CAL. CIV. CODE §§ 1798.100-199 (2020).

Up to twice in twelve months, a business must deliver to the consumer all of the consumer's personal information collected upon a consumer's request.[67] In the context of the CCPA, "personal information" covers a much broader range of information than "personally identifiable information (PII)," a term commonly used in the United States.[68] Put differently, while all PII may be considered personal information, not all personal information is PII.[69]

> As defined by the US Office of Privacy and Open Government, PII is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[70]

To distinguish an individual is to identify an individual by discerning one person from another and to trace an individual is to process sufficient information to determine a specific aspect of an individual's activities or status.[71] Accordingly, one's name, email address, postal address, phone number, and personal ID numbers (e.g., social security, passport, and driver's license) are considered PII.[72]

The CCPA aims to prevent the sale or sharing of California consumers' personal information without their permission, and it protects more than the conventional types of "personal data" such as name, telephone number, and social security number.[73] Under the CCPA, "personal information" includes, but is not limited to, the following if it identifies, relates

[67] Cal. Consumer Prot. Act, CAL. CIV. CODE § 1798.100(d) (2020).
[68] Malia Thuret-Benoist, *What is the difference between personally identifiable information (PII) and personal data?*, TECH GDPR (June 27, 2019), https://techgdpr.com/blog/difference-between-pii-and-personal-data/.
[69] *Id.*
[70] Office of Privacy and Open Government, *Properly safeguarding personally identifiable information (PII) and business identifiable information (PII)*, U.S. Department of Commerce (Accessed 17 April 2020), https://www.osec.doc.gov/opog/privacy/pii_bii.html.
[71] Thuret-Benoist, *supra* note 65.
[72] Thuret-Benoist, *supra* note 64.
[73] Cal. Consumer Prot. Act, CAL. CIV. CODE § 1798

to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

> A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
> B) Any categories of personal information described in subdivision (e) of Section 1798.80;
> C) Characteristics of protected classifications under California or federal law;
> D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
> E) Biometric information;
> F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
> G) Geolocation data;
> H) Audio, electronic, visual, thermal, olfactory, or similar information;
> I) Professional or employment-related information;
> J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99); and
> K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.[74]

Further, the CCPA considers a person's browsing and search history, geolocation data, biometrics, and other types of information that has not been "de-identified" to be worthy of regulation, as well.[75] "Deidentified" means:

> information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information: 1) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; 2) has implemented business processes that specifically prohibit reidentification of the information; 3) has implemented

[74] *Id.* at subdiv. (o)(1)(A–K).
[75] *See id.* at subdiv. (o)(1).

> business processes to prevent inadvertent release of de-identified information; and
> 4) makes no attempt to reidentify the information.[76]

Trade Secret Law Background

A trade secret is information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

> i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[77]

Essentially, trade secrets encompass knowledge of economic commercial value, generated by people who have an interest in protecting their value, in order to gain a competitive economic advantage over other businesses.[78] If a business chooses not to protect its trade secrets, it is likely they will not be considered trade secrets at all.

When it comes to protecting an intellectual asset, businesses must decide whether to protect the intellectual asset with classic Intellectual Property (IP) rights, for example filing for patent or copyright protection, or to keep the asset as a trade secret. Because patents and copyrights only provide a limited monopoly of rights,[79] it may be in the best interests of those who have patentable or copyrightable ideas to keep their secrets rather than to take a limited monopoly. Unlike trademark and copyright law, trade secrets do not require a formal registration process, and unlike

[76] *Id.* at subdiv. (h)(1–4).
[77] UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).
[78] *See id.*
[79] Generally: 20 years from the earliest non-provisional domestic filing date for a utility patent (35 U.S.C. § 154); 15 years from issuance for a design patent (35 U.S.C. § 173); the life of the author plus an additional 70 years for copyright works created after January 1, 1978 (17 U.S.C. § 302); 95 years from the year of its first publication or a term of one hundred and twenty years from the year of its creation, whichever expires first, for an anonymous work, a pseudonymous work, or a work made for hire (17 U.S.C. § 302).

patent law, trade secrets do not require a governmental grant.[80] Instead, trade secrets potentially last forever, protect a broad class of information, and, most importantly, do not require disclosure.[81]

One of the best kept trade secrets in the world is the recipe for Coca-Cola®.[82] Developed by a pharmacist, it has been closely guarded and known to only a few privileged employees for more than 100 years.[83] Coca-Cola® built a successful global brand on it, and competitors have fiercely hunted it.[84] Similarly, Colonel Sanders' secret recipe of 11 herbs and spices for Kentucky Fried Chicken® (KFC®) and the formula for WD-40® are also closely kept secrets that have helped to build their companies' flagship products.[85]

A company can quickly lose its competitive advantage if their trade secrets are improperly managed. Just imagine the level of over-caffeinated law students if someone figured out a way to replicate the secret Coca-Cola® recipe and then shared the formula in what would undoubtedly be a viral YouTube® video. This is why companies go to great lengths to protect their prized secrets. KFC® built a brand new, high-tech safe to safeguard the Colonel's handwritten Original Recipe from 1940.[86] The FireKing® digital safe weighs more than 770 pounds, is encased in two feet of concrete, and has a 24-hour video and motion-detection surveillance system.[87]

---

[80] Atin Basuchoudhary & Nicola Searle, *Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets* (Nov. 2019), available at: https://www.sciencedirect.com/science/article/pii/S0167404819300616.
[81] *Id.*
[82] R. Mark Halligan, *The Secret of Trade Secret Success* (Feb. 9, 2010), available at: https://www.forbes.com/2010/02/19/protecting-trade-secrets-leadership-managing-halligan-haas.html#6ac719de1372.
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*

That level of security is only necessary because the recipe provides KFC with a substantial market advantage. Accordingly, trade secrets generally include any secret information that can provide a company with an advantage in the market; trade secrets may encompass customer identities and pricing information, current research projects, and even failed projects.[88] In the case of WD-40®, the product's name comes from the fortieth try by scientists to come up with a "water displacement" formula for a rust-prevention solvent and degreaser for the aerospace industry.[89] Not only is the WD-40® formula a trade secret, but so are the formulas and work that went into the preceding thirty-nine attempts.[90] Learning about those failed attempts alone would likely save numerous research and development time and expenses for a competitor.[91]

However, it is not enough that confidential information maintains its secrecy; it must also be valuable and derive value from the fact of its secrecy.[92] For instance, Facebook's algorithm that chooses what posts you see and what order those posts are shown in your News Feed is valuable to Facebook because it is secret. Facebook's competitors cannot easily copy the algorithm and offer their own version for use elsewhere—competitors are forced to develop their own algorithms to manipulate the same kind of user data.

Businesses often have no choice but to depend upon the law of trade secrets as a primary source of protection for certain types of valuable business information that they do not want to become public.[93] Previously , the protection provided by the common law of trade secrets and the steps necessary to obtain it were often matters of substantial uncertainty.[94] The choices that courts

[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).
[93] 1 BUSINESS TORTS § 17.05 (2020).
[94] *Id.*

have made between competing policies or various theoretical bases of common law trade secret protection have historically produced inconsistent outcomes.[95] Concern over this variation led to the promulgation of the Uniform Trade Secrets Act ("UTSA").[96] The UTSA is now the single most significant source of controlling trade secret misappropriation law. As of April 2020, forty-eight states as well as Puerto Rico and the U.S. Virgin Islands have adopted either the 1979 or 1985 version of the UTSA.[97] In January 2020, New York also introduced the UTSA to the Senate Judiciary for enactment.[98]

In 1979, the Commissioners on Uniform Laws approved the UTSA and recommended it for adoption in all states.[99] The most significant contribution of the UTSA is the definite focus and structure it provides for the analysis of trade secret claims, including a specific statute of limitations and a statutorily defined cause of action.[100] By its terms, the UTSA displaces all other non-contractual causes of action for relief that are based upon the misappropriation of a trade secret.[101]

A primary purpose of the UTSA is to codify basic principles of common law as enumerated in the better-reasoned court decisions.[102] Concern was also expressed that inconsistency in the

---

[95] *Id.*
[96] *Id.*
[97] Uniform Law Commission, *Trade Secrets Act* (last visited Apr. 9, 2020), available at: https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792.

The UTSA has not been enacted in New York and North Carolina. However, the North Carolina Trade Secrets Protection Act, N.C. GEN. STAT. §§ 66-152 to 66-157 (1981), is in many regards, closely modeled after the UTSA.

The UTSA was enacted in South Carolina in 1992 at S.C. CODE ANN. §§ 39-8-1, 39-8-9 (1996), but was repealed in 1997. *See* 1997 Act No. 38, § 1, effective May 21, 1997. In its place, the South Carolina legislature enacted the South Carolina Trade Secrets Act at S.C. CODE ANN. §§ 39-8-10, 39-8-130 (1997). This Act affords broad trade secret protections in any action, not just misappropriation claims. *See* Hartsock v. Goodyear Dunlop Tires N. Am. Ltd., 422 S.C. 643, 650 (S.C. 2018), citing § 39-8-60. Pursuant to § 39-8-130, this act does not apply to a misappropriation occurring before July 1, 1997, or a continuing misappropriation that began before July 1, 1997.

[98] S. 2468, 2019-2020 Leg., 2019 Reg. Sess. (N.Y. 2019).
[99] UNIF. TRADE SECRETS ACT PREFATORY NOTE (UNIF. LAW COMM'N 1985).
[100] *See id.*
[101] *See* id.
[102] 1 BUSINESS TORTS § 17.05 (2020).

laws of various states was leading to forum shopping.[103] Thus, even in those jurisdictions in which the common law continues to control, decisions under the UTSA may be cited as persuasive authority for the modern view of the principles that govern trade secret misappropriation. [104]

Data As A Trade Secret

Courts have found that virtually any type of information that is capable of being used in a business to obtain a competitive advantage may qualify as a trade secret.[105] Trade secrets can include manufacturing processes, product formulations, plans, blueprints for machines or tools, business plans, or computer programs.[106] Under appropriate circumstances, customer lists also qualify as trade secrets.[107]

Technology companies like Facebook often consider their trade secrets to be the data that they collect, the algorithms that manipulate that data, and the companies to whom they sell that manipulated data (i.e. the data's commercial purpose and their customer lists).[108] Customer lists and other lists related to customer business qualify for trade secret protection if the lists' information cannot be ascertained from other generally available sources.[109] In *Morlife, Inc. v.*

[103] Sharon Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 Hamline Law Rev. 493, 511 (2010).
[104] 1 BUSINESS TORTS § 17.05 (2020).
[105] 1 BUSINESS TORTS § 17.02 (2020).
[106] *Id.*
[107] *Id.*
[108] See generally, Marietje Schaake, *Trade secrets shouldn't shield tech companies' algorithms from oversight*, TECH STREAM (May 4, 2020), https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight/.
[109] Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514, 1521 (1997) (citing Am. Paper & Packaging Prods., Inc. v. Kirgan, 183 Cal. App. 3d 1318, 1326 (1986) (noting that "courts are reluctant to protect customer lists to the extent they embody information which is 'readily ascertainable' through public sources," but that courts recognize as trade secrets customer lists where plaintiff "has expended time and effort identifying customers with particular needs or characteristics"); ABBA Rubber Co. v. Seaquist, 235 Cal. App. 3d 1, 18 (1991) ("A customer list is one of the types of information which can qualify as a trade secret.") (citations omitted); Mattel, Inc. v. MGA Entm't, Inc., 782 F. Supp. 2d 911, 972 (C.D. Cal. 2010) (noting that client lists have potential or actual value from not being generally known to the public: information about customers' preferences can aid in "securing and retaining their business) (citing

Perry, the California Court of Appeals held that customer identities from an organization's list are protected as trade secrets if the identities are not generally known to the industry.[110] The court also found three factors to be helpful when determining whether reasonable efforts have been made to qualify something as a trade secret: (1) how the entity stores the information; (2) who has access to the information; and (3) whether the information was subject to confidentiality provisions.[111]

In *Morlife*, the court ruled that information about customers that was "stored on a computer with restricted access" which had been subject to a confidentiality provision expressly referring to customer names and telephone numbers was subject to trade secret protection.[112] According to *Morlife*, information that is difficult and time-consuming to obtain will likely be more protectable than information that was neither difficult nor time-consuming to obtain.[113] Further, courts have noted that information including customer lists and contact information, pricing guidelines, historical purchasing information, and customers' business needs or preferences typically receives trade secret protection as it has potential or actual value from not being generally known to the public.[114]

It has been long held that certain data can be a trade secret when correctly protected.[115] A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives one an opportunity to obtain an advantage over competitors

Aetna Bldg. Maint. Co. v. West, 246 P.2d 11, 16 (Cal. 1952)).
[110] *See Morlife*, 56 Cal. App. 4th at 1522.
[111] *See id.* at 1523.
[112] *Id.*
[113] *See id.* at 1522–1523.
[114] Brocade Commc'n Systems Inc. v. A10 Networks Inc., 873 F.Supp.2d 1192, 1214–1215 (N.D. Cal. 2012); *See, e.g.*, *ABBA*, 235 Cal. App. 3d at 18 ("A customer list is one of the types of information which can qualify as a trade secret.") (citations omitted). This information has potential or actual value from not being generally known to the public: information about customers' preferences can aid in "securing and retaining their business." Mattel, Inc. v. MGA Entm't, Inc., 782 F. Supp. 2d 911, 972 (C.D. Cal. 2011) (citing Aetna Bldg. Maint. Co. v. West, 246 P.2d 11, 16 (Cal. 1952)).
[115] Kewanee v. Bicron, 416 U.S. 470, 499 (1974).

who do not know or use it.[116] The Supreme Court has also held that customer lists qualify as trade secrets.[117] Other jurisdictions also note that customer-related information, including customer lists and contact information, pricing guidelines, historical purchasing information, and customers' business needs or preferences, are routinely given trade secret protection.[118] This type of information has potential or actual value from not being generally known to the public: information about customers' preferences can aid in securing and retaining their business.[119]

Yet, there has been debate on how a customer list qualifies for trade secret protection. California courts have found that a company can establish protectable trade secrets in its customer lists and customer preferences when holders expend time and effort identifying customers with particular needs or characteristics.[120] In *Sun Distributing Company LLC v. Corbett, the* court held that "the value to the customer list is in the completeness and details of the list; the fact that each individual customer has access to its own information does not make Plaintiff's list of customers worthless."[121] The court also rejected the argument that the publisher information was publicly available and therefore not protectable, reasoning that although publication names and contact information might be public knowledge, it was clear that Sun Distributing had put in time and effort to develop other specific information, including its customer lists, preferences, pricing structures, and "do not deliver" lists.[122]

Conversely, the court in *American Paper & Packaging Products, Inc. v. Kirgan* held that a customer list was not protected as a trade secret because it was known or readily ascertainable to

[116] *Id.* at 474-475.
[117] *Id.* at 475.
[118] *See Brocade Commc'n*, 873 F. Supp. 2d at 1214–1215.
[119] *Id.* at 1214 (quoting Mattel, Inc. v. MGA Entm't, Inc., 782 F. Supp. 2d 911, 972 (C.D. Cal. 2010) (citing Aetna Bldg. Maint. Co. v. West, 246 P.2d 11, 16 (Cal. 1952)).
[120] Sun Distrib. Co., LLC v. Corbett, No. 18-CV-2231, 2018 U.S. Dist. LEXIS 176224, at *11 (S.D. Cal. Oct. 12, 2018).
[121] *Id.*
[122] *Id.*

other persons in the competitive business of shipping, and the compilation process at issue was neither sophisticated, difficult, nor particularly time-consuming.[123] Sometimes overlooked in the context of marketing efforts, companies often list representative customers as a business development tool on their websites and in other pubic arenas. As a general rule, a company should not publicly disclose information it is trying to keep secret.[124]

Because this paper focuses on the California Consumer Privacy Act, it also focuses on California trade secret law. Like the majority of states, California has adopted a version of the UTSA.[125] Thus, much of California's trade secret law mirrors that of other UTSA states. One notable difference, however, is in the definition of a trade secret that does not include the "readily ascertainable" requirement.[126] However, the "readily ascertainable" issue still comes up in California cases. The assertion that a matter is readily ascertainable by proper means is available as a defense to a claim of misappropriation instead of being a burden on the plaintiff to disprove that the information in question is readily ascertainable.[127]

Concerning the general availability of customer information, courts are reluctant to protect customer lists to the extent they embody information that is "readily ascertainable" through public sources, such as business directories,[128] particularly because it is a requirement under the UTSA that information not be readily ascertainable to receive trade secret protection.[129] However, where a holder has expended time and effort identifying customers with particular needs or

[123] Am. Paper & Packaging Prods. v. Kirgan, 183 Cal. App. 3d 1318, 1326 (1986).
[124] Veronica Foods Co. v. Ecklin, No. 16-CV-07223-JCS, 2017 WL 2806706, at *14 (N.D. Cal. June 29, 2017) (declining to find a trade secret where a company disclosed at least some of its customers and suppliers on its website).
[125] CAL. CIV. CODE §§ 3426-3426.11 (1984).
[126] *Id.*
[127] DVD Copy Control Ass'n, Inc. v. Bunner, 31 Cal. 4th 864, 899 (2003).
[128] Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514, 1521 (1997), *see supra* parenthetical text accompanying note 103, at 21.
[129] UNIF. TRADE SECRETS ACT § 1(4)(i) (UNIF. LAW COMM'N 1985).

characteristics, courts will prohibit misappropriation of this information to capture a share of the market.[130] It is this combination of elements that makes the information valuable and not generally known to the public.[131] Such lists are to be distinguished from mere identities and locations of customers where anyone could easily identify the entities as potential customers.[132]

Even when a court finds that customer information is not generally known or readily ascertainable, the UTSA requires that the information also have independent economic value.[133] The fact that the same information can be gathered on any one customer by talking with the customer herself is irrelevant.[134] The value in a company's customer information is in the compilation, categorization, and organization of information on customers, combined with the ability to search and format it into a readily usable form.[135] Competitors do not have and cannot easily recreate the organization of this kind of information.[136]

A simple list of customers may not necessarily be a trade secret in that the identities of the customers could readily be determined by examining any directory.[137] Information has independent economic value and is held to be a trade secret when, for example, a database includes the primary contact at each customer, the pricing and discounts for the customer's past contracts with competitors, the customer's payment terms, where and how frequently that customer has published advertisements in the past, the customer's past complaints and requests, and the customer's personal information.[138]

---

[130] *See Morlife*, 56 Cal. App. 4th 1514 at 1521, *supra* accompanying text note 122.
[131] Brocade Commc'n. Sys. v. A10 Networks, Inc., 873 F. Supp. 2d 1192, 1215 (N.D. Cal. 2012).
[132] *See Morlife*, 56 Cal. App. 4th 1514 at 1521, *supra* accompanying text note 122.
[133] UNIF. TRADE SECRETS ACT § 1(4)(i) (UNIF. LAW COMM'N 1985).
[134] *See Morlife*, 56 Cal. App. 4th 1514 at 1526.
[135] *See generally id.*.
[136] *Id.*
[137] W. Directories, Inc. v. Golden Guide Directories, Inc., No. C 09-1625 CW, 2009 U.S. Dist. LEXIS 52023, at *14 (N.D. Cal. June 8, 2009).
[138] *Id.* at 13-14.

The subject of a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business.[139] However, this necessary element of secrecy is not lost if the holder of the trade secret reveals the trade secret to another "in confidence, and under an implied obligation not to use or disclose it."[140] Disclosure to “another” may include those of the trade secret holder's "employees to whom it is necessary to confide it, in order to apply it to the uses for which it is intended."[141] A trade secret holder’s licensee is often the recipient of confidential knowledge of the subject of a trade secret.[142]

The protection accorded to a trade secret holder is against the disclosure or unauthorized use of the trade secret by those to whom the secret has been confided under the express or implied restriction of nondisclosure or nonuse.[143] The law also protects the holder of a trade secret against disclosure or use when the knowledge is gained, not by the owner's volition, but by some "improper means," which may include theft, wiretapping, or even aerial reconnaissance.[144] However, trade secret law does not offer protection against discovery by fair and honest means; for example, by independent invention, accidental disclosure, or reverse engineering.[145]

Curiously, trade secret law is a two-way street: It protects confidential ideas, but it also requires giving notice that the information is in fact a secret so that others do not use information that they think is not confidential.[146] An implied duty of confidentiality may be found when the other party has reason to know that the information was in fact confidential.[147] For example, the

[139] B. F. Goodrich Co. v. Wohlgemuth, 192 N.E.2d 99, 104 (Ohio Ct. App. 1963); National Tube Co. v. Eastern Tube Co., 3 Ohio C.C.(N.S.) 459, 462 (1902), aff'd, 69 Ohio St. 560 (1903).
[140] Cincinnati Bell Foundry Co. v. Dodds, 10 Ohio Dec. Reprint 154, 156 (Ohio 1887).
[141] *National Tube*, 3 Ohio C.C.(N.S.) 459 at 462.
[142] *See* Lear, Inc. v. Adkins, 395 U.S. 653, 655 (1969).
[143] Kewanee v. Bicron, 416 U.S. 470, 475 (1974).
[144] *Id.* at 475-476.
[145] *Id.*.at 476.
[146] Carr v. AutoNation, Inc., No. 19-15408, 2020 U.S. App. LEXIS 7840, *2 (9th Cir. Mar. 12, 2020).
[147] *Id.* at *3.

court in *Carr v. AutoNation, Inc.* held that the appellant failed to take reasonable efforts to maintain the secrecy of his business plan when he sent the business plan to (among others) appellee's founder, failed to label the business plan as confidential, never told appellee that the information was confidential, and did not seek a non-disclosure agreement before sending the plan.[148] Thus, even when a trade secret is disclosed to an employee, licensee, or the like, a holder must still make reasonable efforts to maintain its secrecy.[149]

Furthermore, the way in which publicly available information is combined, compiled, and integrated has been held to entitle the resulting product to protection as a trade secret, given the right set of facts.[150] In *United States v. Nosal*, the federal government (plaintiff) prosecuted David Nosal (defendant) for trade-secret theft, in violation of 18 U.S.C. § 1832.[151] Nosal was employed by Korn/Ferry International, a corporate executive-search firm.[152] Korn/Ferry's key asset was its proprietary "Search" database, containing data on thousands of potential corporate executives.[153] The data was uploaded from public sources such as LinkedIn.[154] Search's value to Korn/Ferry was derived from its capability to aggregate previous user queries and the outcomes of previous executive searches to refine its capability to generate targeted candidate search lists.[155] Korn/Ferry never gave anyone access to Search without making them sign strict confidentiality agreements, which emphasized Search's valuable and legally protected status.[156] The Search home screen notified users that it was "intended to be used by Korn/Ferry employees

[148] *Id.*
[149] UNIF. TRADE SECRETS ACT § 1(4)(ii) (UNIF. LAW COMM'N 1985).
[150] *See generally* United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016).
[151] *Id.* at 1041.
[152] *Id.* at 1030.
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] *Id*. at 1031.

for work on Korn/Ferry business only," and search lists generated by Search were marked "Korn/Ferry Proprietary & Confidential."[157]

Nosal and several associates secretly downloaded Search data to help them establish a rival executive-search company.[158] Even after Nosal and his associates quit Korn/Ferry and set up their own business, they persuaded an ally still on the Korn/Ferry payroll to continue funneling Search data to them.[159] A jury convicted Nosal of trade secret theft; Nosal appealed and argued that Search data could not be considered a trade secret because it came from public sources, that Korn/Ferry shared Search data with others, and that Nosal neither knew nor intended that his unauthorized use of Search data would hurt Korn/Ferry.[160]

Yet, the Ninth Circuit Court of Appeals affirmed Nosal's conviction of trade secret theft, noting that the way in which publicly available information is combined, compiled, and integrated can entitle the resulting product to protection as a trade secret.[161] Nosal's argument that Korn/Ferry shared Search data with others was contradicted by evidence, such as the mandatory confidentiality agreement that Nosal signed, and the fact that Korn/Ferry took aggressive measures to deter unauthorized access to Search.[162] Given Nosal's confidentiality agreement and the prominent warnings on Search's home screen and search lists, it is naive to think that Nosal was unaware that unauthorized access to Search would injure Korn/Ferry.[163]

The Court held that publicly available data can form the basis of a trade secret if a business invests its own effort and creativity to create a product that exploits the data in such a way as to

[157] *Id.* at 1044.
[158] *Id.* at 1031.
[159] *Id.*
[160] *Id.*
[161] *Id.* at 1029.
[162] *Id.* at 1043.
[163] *Id.* at 1044.

make it uniquely valuable to the business, and then aggressively protects the product from unauthorized use.[164]

Conclusion

The challenge that the CCPA now places on businesses is how to comply with consumer privacy disclosure requirements while also complying with trade secret confidentiality requirements. Requiring companies to disclose the "business or commercial purpose for collecting or selling personal information"[165] essentially necessitates companies to disclose how or why their trade secrets give them a market advantage by providing lists of the types of manipulated data that they are selling as well as lists of who they sell that manipulated data to. Further, the "categories of third parties with whom the business shares personal information"[166] is comparable to a client list, which is a well-established trade secret right.[167]

One way that businesses can potentially prevent their trade secrets from being disclosed under the CCPA is by de-identifying their consumers' "personal information" as defined by the CCPA. If companies de-identify their consumers' personal information, consumers then would only be able to access data strictly related to their biographical information, and trade secret holders would be free not to disclose the output of their data processing (behavior evaluation, forecast, studies on life expectancy, personalized marketing plan, pricing, etc.).[168]

[164] *Id.* at 1043.
[165] CAL. CIV. CODE § 1798.110 (a)(3)(Deering 2020).
[166] CIV. § 1798.110(a)(4).
[167] If the lists' information cannot be ascertained from other generally available sources. *See* Morlife Inc. v. Perry, 56 Cal. App. 4th 1514, 1522 (1997); ABBA Rubber Co. v. Seaquist, 235 Cal. App. 3d 1, 20 (1991); Mattel, Inc. v. MGA Entm't, Inc., 782 F. Supp. 2d 911, 1018 (C.D. Cal. 2010).
[168] GIANCLAUDIO MALGIERI, *TRADE SECRETS V. PERSONAL DATA: A POSSIBLE SOLUTION FOR BALANCING RIGHTS*, Vol. 6, No. 2, INTERNATIONAL DATA PRIVACY LAW, 102-116, 112 (2016).

To the extent that any of the information a company must disclose under the CCPA is a trade secret, there is another potential conflict between the goals of the CCPA and the protections provided to certain information by California's version of the UTSA. The CCPA could limit the protection of potential trade secret information in California as the information either needs to be a trade secret or protected by contract; all other tort claims do not exist.[169]

As previously noted, the UTSA displaces all other non-contractual causes of action for relief that are based on the misappropriation of trade secrets.[170] Under California's Uniform Trade Secrets Act ("CUTSA"), a party may recover for the "actual loss" or other injury caused by the misappropriation of trade secrets.[171] CUTSA defines misappropriation as (1) the improper acquisition of a trade secret or (2) the non-consensual disclosure or use of a trade secret.[172]

CUTSA provides an exclusive civil remedy for conduct falling within its terms, and courts have reasoned that it displaces common law tort claims in two circumstances.[173] First, CUTSA displaces claims that are "based on the same nucleus of facts as the misappropriation of trade secrets claim for relief."[174] Stated differently, CUTSA displaces tort claims where they "do not genuinely allege 'alternative legal theories' but are a transparent attempt to evade the strictures of CUTSA by restating a trade secrets claim as something else."[175]

Second, CUTSA displaces "all claims premised on the wrongful taking and use of confidential business and proprietary information, even if that information does not meet the

[169] UNIF. TRADE SECRETS ACT PREFATORY NOTE (UNIF. LAW COMM'N 1985).
[170] *Id.*
[171] CIV. § 3426.3.
[172] *Id.* at § 3426.1(b).
[173] Erhart v. Bofi Holding, Inc., No. 15 CV 02287, 2020 U.S. Dist. LEXIS 57137, at *102 (S.D. Cal. Mar. 31, 2020); Yet, not all states follow Section 7 of the UTSA (Iowa Code § 550.1-550.8 (2018)).
[174] *Erhart.* 2020 U.S. Dist. LEXIS 57137, at *102 (quoting K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc., 90 Cal. Rptr. 3d 247, 261 (Cal. Ct. App. filed March 3, 2009)).
[175] *Id*. (quoting Silvaco Data Sys. v. Intel Corp., 109 Cal. Rptr. 3d 27, 54 (Cal. Ct. App. filed April 29, 2010); *see also K.C. Multimedia*, 90 Cal. Rptr. 3d 247 at 262–264 (concluding CUTSA displaced breach of confidence, interference with contract, and unfair competition claims)).

statutory definition of a trade secret."[176] A primary purpose of the UTSA "was to sweep away the adopting states' bewildering web of rules and rationales and replace it with a uniform set of principles for determining when one is and is not liable for acquiring, disclosing, or using 'information . . . of value.'"[177] "Information that does not fit" the definition of a trade secret, "and is not otherwise made property by some provision of positive law, belongs to no one, and cannot be converted or stolen."[178] Thus, if the basis of the alleged property right is in essence that the information is not generally known to the public, then the claim is sufficiently close to a trade secret claim that it should be superseded notwithstanding the fact that the information fails to meet the definition of a trade secret.[179]

While the appellant in *Erhart v. Bofi Holding, Inc.* did not plead a trade secret misappropriation claim, the court held that BofI's tort claims implicated trade secret principles.[180] The gravamen of BofI's tort claims was that Erhart wrongfully accessed and took its "confidential and proprietary information."[181] BofI also repeatedly used the terms "misappropriate" and "misappropriation" in its pleading.[182] By not pleading a trade secret misappropriation claim, BofI attempted to evade CUTSA's requirements, including proving that the information rises to the level

[176] *Erhart.* 2020 U.S. Dist. LEXIS 57137, at *102 (quoting ChromaDex, Inc. v. Elysium Health, Inc., 369 F. Supp. 3d 983, 989 (C.D. Cal. 2019)); *accord* Copart, Inc. v. Sparta Consulting, Inc., 277 F. Supp. 3d 1127, 1158 (E.D. Cal. 2017); Mattel, Inc. v. MGA Entm't, Inc., 782 F. Supp. 2d 911, 987 (C.D. Cal. 2011).
[177] *Erhart.* 2020 U.S. Dist. LEXIS 57137, at *102 (quoting *Silvaco*, 109 Cal. Rptr. 3d 27 at 53 n.22).
[178] *Id*.
[179] *Id.* (quoting SunPower Corp. v. SolarCity Corp., No. 12 CV 00694, 2012 U.S. Dist. LEXIS 176284, 2012 WL 6160472, at *5 (N.D. Cal. Dec. 11, 2012) (citing CAL. CIV. CODE § 3426.1(d)(1)).
[180] *Id.* at *104.
[181] *Id.*
[182] *Id*.

of a protectable trade secret.[183] Yet, BofI still sought to impose liability on Erhart for "acquiring, disclosing, or using" confidential information of purported value.[184]

Given this conduct, BofI argued CUTSA does not displace BofI's tort claims that pursued Erhart for the damages it incurred to recover this sensitive information and prevent unauthorized disclosures.[185] The court felt that this argument had merit as BofI had an obligation to protect the nonpublic personal information of its customers.[186] In this sense, BofI's allegations concerning Erhart's unauthorized taking of customer financial information were more akin to a data breach claim than a disguised trade secrets claim.[187] In the same vein, the Court found distinguishable BofI's allegation that Erhart wrongfully took nonpublic personal information of BofI's employees, such as BofI's CEO's personal tax returns.[188] For CUTSA displacement, the Court found that there was a meaningful distinction between BofI's efforts to safeguard this information, as compared to BofI's efforts to impose liability on Erhart for wrongfully taking "information containing BofI's intellectual property" and the Bank's "confidential and proprietary information."[189]

If, as the foregoing suggests, some of the information that database owners collect and manipulate can be protected as a trade secret under California law, then a related question is whether there are any circumstances that can require disclosure of the trade secret to either the general public or governmental regulatory authorities. In an unpublished California case, the Court

[183] *See* CAL. CIV. CODE § 3426.1(d) (Deering 2020).
[184] *Erhart.* 2020 U.S. Dist. LEXIS 57137, at *104. (*See Silvaco*, 184 Cal. App. 4th at 239 n.22.)(*See also* BofI's Opp'n 16:3-5 (arguing "there was value in the information Erhart converted because BofI invested time and expense in creating, [*105] assembling, and maintaining its data")).
[185] *Id.* (*See* BofI's Opp'n 6:21-7:6; 14:17-19.)
[186] *Id* at *107.
[187] *Id.* (citing *K.C. Multimedia*, 171 Cal. App. 4th at 958) (quoting *ChromaDex*, 369 F. Supp. 3d at 989) ("…or claim premised on the wrongful taking and use of confidential business and proprietary information.")
[188] *Id.* (*See* BofI's FAC ¶ 11; Erhart Dep. 639:7-640:14, ECF No. 155-3; Ball Dep. 318:7-18, ECF No. 155-6).
[189] *Id.* at *96. (*See* BofI's FAC ¶ 11.) Cf. CTC Real Estate Servs. v. Lepe, 140 Cal. App. 4th 856, 860, 44 Cal. Rptr. 3d 823 (2006) (noting that one's personal identifying information "is a valuable asset" because its misuse "can have serious consequences to that person" and it can be the object of theft)).

of Appeals held that a defendant is not entitled, prima facie, to the trade secret source code of a DNA program used to identify the defendant.[190] Shelley H. was murdered in 1977, and a forensics agency later conducted a DNA test on swabs taken from Shelley in 2011.[191] The DNA sample was found to be a match for Martell Chubbs, who was subsequently arrested and tried for murder.[192]

Chubbs filed a motion to compel discovery of the source code used in the software program that identified Chubbs.[193] The plaintiff government of California, on behalf of the developer of the software, filed an opposition motion, arguing that the source code was a protected trade secret and that disclosure of the code would be financially devastating for the developer.[194] Chubbs countered that the source code was essential to his defense because the DNA evidence was the only evidence against him.[195] Without the source code, Chubbs claimed, there would be no way for Chubbs to determine what assumptions were made regarding the evidence and if those assumptions were appropriate.[196] The developer of the software testified that the source code was not needed to assess the program's reliability, and that publicly revealing the source code would allow competitors to easily copy the program.[197]

The *C*ourt held that Chubbs was not entitled to the source code of the DNA program used to identify Chubbs for the murder of Shelly H.; the owner of a trade secret has a privilege to refuse to disclose the secret if the allowance of the privilege would not tend to conceal fraud or otherwise work injustice.[198] Once the existence of a trade secret has been established, the party seeking discovery must make a prima facie, particularized showing that the information sought is relevant

[190] People v. Superior Court (Chubbs), No. B258569, 2015 WL 139069, *9 (Cal. Ct. App. Jan. 9, 2015).
[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] *Id.* at *3.
[196] *Id.*
[197] *Id.* at *4.
[198] *Id.* at *5.

and necessary to a material element of a cause of action in the case.[199] "[I]t is not enough that a trade secret might be useful to real parties."[200]

Unlike the criminal charge in *Chubbs*, a burden-shifting procedure is used to evaluate assertion of the trade secret privilege in civil cases.[201] However, similar to the holding in *Chubbs*, requiring companies to disclose their trade secrets under the CCPA without a prima facie, particularized showing that the information sought is relevant and necessary to a cause of action will give consumers a way to easily copy trade secret material. California is already a largely technology-driven state, so when consumers start requesting companies to disclose information about how the consumers' personal information is collected, used, shared, or sold, trade secret material will spread like wildfire. Mandating businesses to disclose their trade secret data to consumers is problematic when courts do not require businesses to disclose trade secrets like source code for a DNA test which could potentially convict someone of first-degree murder—arguably a much more serious offense than a general right of privacy claim.

While the point of the CCPA is to provide consumers with privacy rights as they relate to businesses' use of consumers' data, it is also debatable whether consumers have a reasonable expectation of privacy for information that they themselves have already held out to a third party.[202] Take a Facebook user's profile, for example. No matter the privacy settings, a user is holding out at least some information to third parties—those third parties could the general Facebook public, or "friends of friends" tagged in a photo, perhaps. Depending on her privacy settings, if Facebook user Laura posts a photo and tags her friend Daniel in it, Daniel's friend

[199] *Id.*
[200] *Id.* at *9 (quoting Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709 (1992)).
[201] *Id.*
[202] United States v. Miller, 425 U.S. 435, 442-443 (1976) (holding that held that bank customers have no reasonable expectation of privacy in their bank records because bank customers voluntarily give any information contained in bank records to the bank and such records are observable by the bank's employees).

Aimee can see Laura's post even though Laura and Aimee are not "friends." Although Laura may not normally be holding out information to Aimee as a third party, she has done so in this instance.

Laura would have an unreasonable expectation of privacy in the scenario above. Yet, under the CCPA, Laura could require Facebook to disclose to her what third parties Facebook sold her data to even though she has already held the information out to third parties herself.

Another perspective to consider is that trade secrets are part of the privacy area of legal persons. Even if the information that a consumer once provided to a company is still considered a property right of the consumer, the consumer most certainly does not own the innovative technique of how a company uses the consumer's data in an algorithm or forecasting model, for example. Trade secret protection is not based on a piece of information but is based on the confidentiality behind that information.[203] After all, trade secrets are generally considered personal data of businesses because they represent private data related to the intimacy of the legal person.[204] Trade secrets are not just a form of intangible asset of a company, but they are a form of protection of personality rights of the businessperson and her employees.[205] Therefore, if the law also protected legal persons' personal data, the conflict between trade secret rights and data protection rights thus becomes a conflict between a natural persons' data protection (the consumers) and a legal persons' data protection (the company).[206]

The issue ultimately comes down to which is more important—personal privacy or trade privacy? One could argue that legal entities should not be considered as data subjects because they already benefit from the protection of other sectors of the law like trade secrets, unfair competition,

[203] GIANCLAUDIO MALGIERI, *TRADE SECRETS V. PERSONAL DATA: A POSSIBLE SOLUTION FOR BALANCING RIGHTS*, Vol. 6, No. 2, INTERNATIONAL DATA PRIVACY LAW, 102-116, 112 (2016).
[204] *Id.* at 108.
[205] *Id.* at 115.
[206] *Id.* at 108.

trademarks, and patents.[207] On the other hand, trade secrets are a large part of what gives a company a competitive edge and what drives interstate commerce, which undoubtedly provides the federal government with a vested interest in helping to keep trade secrets confidential.[208]

Requiring disclosure of trade secret information to a consumer is almost sure to result in the misappropriation of trade secrets because consumers have no obligation to keep a businesses' trade secrets confidential. Suppose that, under the CCPA requirements, Apple® discloses to consumer Julie Smith to whom and how her data is sold. Consumer Julie happens to work at a competitor, Samsung. Julie could then easily disclose Apple's trade secret to Samsung in her normal line of work. Because Julie has no obligation under an employment agreement with Apple to keep Apple's trade secret confidential, Apple would likely have no recourse for trade secret misappropriation under CUTSA. Further, because Apple had to "voluntarily" disclose the trade secret to Julie under the CCPA, it could be difficult to argue that Apple made reasonable efforts to maintain the secrecy to keep its trade secret confidential.

Requiring every consumer who requests information about their data usage under the CCPA to sign a Non-Disclosure Agreement (NDA) is one idea to help businesses show that they have made efforts that are "reasonable under the circumstances to maintain the secrecy of their trade secrets."[209] However, obtaining every single consumers' signature on an NDA would be burdensome for businesses. Further, the CCPA explicitly states that a business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights,[210]

---

[207] *Id.*
[208] *See* U.S. Const. art. I, § 8, cl. 3., which gives Congress the power "to regulate commerce with foreign nations, and among the several states."; *See also* Wickard v. Filburn, 317 U.S. 111, 125 (1942) (holding that the federal power to regulate production of goods for commerce is commerce if it has a "substantial economic effect" on interstate commerce and that commerce is nationally significant in its cumulative effect, such as altering the supply-and-demand relationships in the interstate commodity market).
[209] UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).
[210] CAL. CIV. CODE § 1798.125 (Deering 2020).

so requiring every consumer to sign an NDA to receive information about the use of their data may be considered a discriminatory or coercive practice in that it imposes additional obligations on the consumer to receive the data they are requesting. Requiring NDA's would also be against the public policy of the CCPA in general.

While some remedies may exist to limit the disclosure of trade secrets under the obligations of the CCPA, none are all-encompassing, and the success of any remedies is yet to be seen due to the recency of the law. Moreover, as each state enacts legislation similar to the CCPA, the tangled web of compliance will continue to spin.

Cybaris®

Cybaris®, an Intellectual Property Law Review, publishes non-student articles and student comments on all areas of intellectual property law, including patents, copyrights, trademarks, licensing, and related transactional matters.
mitchellhamline.edu/cybaris

Intellectual Property Institute

Cybaris® is a publication of the Intellectual Property Institute at Mitchell Hamline School of Law.
mitchellhamline.edu/ip

MITCHELL | HAMLINE
School *of* Law

875 Summit Avenue, Saint Paul, MN 55105
mitchellhamline.edu