WHAT IS MY SELF-WORTH? AN ANALYSIS OF CALIFORNIA'S STATUTORY PROTECTIONS FOR PERSONAL INFORMATION

INTRODUCTION

In the state of California, "unfair competition" and "unfair business practices" are defined statutorily under the California Business and Professional Code, Section 17200 (the UCL). The UCL states, in part, "As used in this chapter, unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising . . . ."[1]

Notably, this language does not directly provide insights into what practices may constitute unfair competition. Hence, California common law has historically illuminated which disputes have standing under the UCL.

The UCL cause of action is available to any "person who has suffered injury in fact and has lost money or property as a result of the unfair competition."[2] The California Supreme Court has clarified that the phrase "injury in fact" is a "legal term of art" coming from Article III, Section 2 federal standing requirements.[3] "Under federal law, injury in fact is 'an invasion of a legally protected interest which is (a) concrete and particularized; and (b) "actual or imminent, not conjectural or hypothetical."'"[4] However, case law coming out of the Northern District of California reveals that what constitutes "unfair business practices" is still up for debate in the realm of internet privacy.[5]

As the first of its kind to be heard under the UCL, *In re Facebook Privacy Litigation*[6] reached the U.S. District Court for the Northern District of California in 2011, in which a putative class action challenged technology giant Facebook (now Meta Platforms), alleging that the defendant's sale of personal data constituted unfair competition.[7] According to the plaintiffs, Facebook's own policies

1. CAL. BUS. & PROF. CODE § 17200 (2026).
2. *Id.* § 17204.
3. *See* Kwikset Corp. v. Superior Ct., 246 P.3d 877, 885 (Cal. 2011).
4. *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).
5. *See, e.g.*, *In re* Facebook Priv. Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011); *but see* Brown v. Google LLC, No. 20-CV-03664, 2021 WL 6064009, at *14–15 (N.D. Cal. Dec. 22, 2021).
6. 791 F. Supp. 2d 705 (N.D. Cal. 2011).
7. *Id.* at 708.

prohibit the revelation of user identity or personal information to advertisers.[8] However, when Facebook users clicked on an advertisement, the advertisers would get a "Referrer Header" which would reveal the last webpage the users looked at prior to clicking on the ad—often the individuals' profiles that contained their personal information.[9]

The plaintiffs argued that Facebook "intentionally and knowingly transmitted personal information about [them] to third-party advertisers without [their] consent."[10] The court rejected this claim, concluding that the plaintiffs lacked standing since they did not allege a loss of money or property, thereby failing the UCL requirements.[11] It specifically noted that "[t]o assert a UCL claim, a private plaintiff needs to have 'suffered injury in fact and . . . lost money or property as a result of the unfair competition.'"[12] Furthermore, a plaintiff's personal information does not constitute property under the UCL.[13] Therefore, the *Facebook* line of reasoning effectively barred future suits under the UCL pursuant to a theory of harm to personal data.

However, a decade later the court reexamined the question of whether a personal data injury is viable under the UCL in *Brown v. Google*.[14] The plaintiffs were Google account users who, relying on the Google Privacy Policy, believed that their data would not be tracked when using a private browser, called "incognito mode."[15] These representations included statements assuring that Chrome would not store certain information, such as snapshots of pages visited, records of downloads, or "basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites [visited]."[16] In addition, the Chrome Privacy Notice stated, "Chrome won't share existing cookies with sites you visit in incognito or guest mode."[17]

In the complaint, the plaintiffs alleged that Google's practice of "using its advertising and data analytics services to collect data from internet users who visit websites"[18] while in incognito mode violated

8. *Id.* at 709.
9. *Id.*
10. *Id.* at 708.
11. *Id.* at 710.
12. *Id.* at 714 (quoting Rubio v. Cap. One Bank, 613 F.3d 1195, 1203 (9th Cir. 2010) (alteration in original)).
13. Thompson v. Home Depot, Inc., No. 07cv1058, 2007 WL 2746603, at *3 (S.D. Cal. Sep. 18, 2007).
14. Brown v. Google LLC, No. 20-CV-03664, 2021 WL 6064009 (N.D. Cal. Dec. 22, 2021).
15. *Id.* at *11–12.
16. *Id.* at *14.
17. *Id.*
18. *Id.* at *4–5.

the UCL.[19] Arguing on a theory of unlawfulness, the plaintiffs specifically alleged a violation of the Federal Wiretap Act, among other statutes.[20] Unlike the court in *Facebook*, this court held that the browser's data collection practice did cause a UCL violation and injury because the plaintiffs provided valuable data to Google and received no money in return.[21] In doing so, the court rejected the *Facebook* requirement that plaintiffs must demonstrate actual monetary or property loss.

How did California's Northern District Court go from *Facebook* to *Brown* in just ten years? Is the divergence of case law due to a shift in cultural understandings and attitudes toward big tech companies selling personal information? Or is the change simply due to plaintiffs growing more artful in their pleadings? Should data privacy be governed under the UCL at all? Can the UCL be reformed to remedy its defects?

This Comment begins with an exploration of what California considers to be unfair competition and how unfair competition laws are analyzed outside the realm of data privacy in Part I. Part II asks and answers whether the UCL recognizes personal information as property and whether this information can be an injury-in-fact. It does so by tracing the historical development of caselaw from the Northern District of California to determine (1) how infringements on data privacy are treated under the UCL and (2) why *Facebook* and *Brown* differ despite an unchanged legal standard.

Part III then argues that changes in federal pleading standards in the first decade of the twenty-first century have likely been determinative of whether a UCL plaintiff is subject to dismissal. It concludes that artful pleading, rather than the merits of the claim, has been the harbinger of success for personal information claims under the UCL.

Part IV evaluates California's statutory reforms, positing that data infringement claims are better litigated under California's Consumer Privacy Act (the CCPA) to avoid the UCL's seemingly arbitrary, fact-intensive analysis and prevent the possibility of divergent outcomes in similar claims such as that between *Facebook* and *Brown*. However, Part V identifies statutory deficiencies in both the UCL and the CCPA, concluding that neither statute provides enough bite for litigants. To remedy this, this Comment proposes: (1) establishing a rebuttable presumption for UCL plaintiffs that there has been an injury in fact to personal data as property; or (2) affording CCPA plaintiffs a private right of action.

Part VI looks beyond the current UPL and CCPA to the future of data privacy litigants in the age of artificial intelligence, ultimately

19. *Id.* at *43.
20. *Id.* at *43–44.
21. *Id.* at *52.

concluding that although California has taken measures to protect consumers, the growth of such intelligence requires ever-changing policing to enforce an ever-changing system.

I. WHAT IS THE UCL?

The UCL allows plaintiffs an equitable alternative to traditional contract disputes. Instead of arguing breach of contract, which often requires memorialized writings with explicit promises (that often do not exist), plaintiffs instead must make a showing of unlawful, unfair, or fraudulent practices.[22] As stated by the court in *In re Anthem, Inc. Data Breach Litigation*,[23] under a breach of contract claim, California plaintiffs must do something more than "merely point to allegations of a statutory violation."[24] However, under the UCL, plaintiffs do not need to do *anything more* than allege unlawfulness. "'By proscribing any unlawful business practice,' the UCL 'borrows violations of other laws and treats them as unlawful practices that the UCL makes independently actionable.'"[25] Another notable difference between contract law and the UCL is that the UCL provides three separate theories of liability: the "unlawful, the unfair, and the fraudulent prong."[26] Therefore, claims under the UCL have the potential to reach outside the scope of any contractual breach.

The UCL is additionally limited in its available remedies. Although the UCL covers a plethora of actions that are "unfair," its remedies lie only in equity. Therefore, where a plaintiff seeking monetary damages may look to contract law for relief, those affected by unfair practices regarding their personal information may want to seek equitable relief, whether it be for the purpose of improving corporate disclosure or preventing additional data breaches. Furthermore, these plaintiffs may not even be able to quantify their harm in any dollar amount, thus preventing a showing of damages under contract law.

While on its face the UCL seems entirely appropriate for remedying breach of contract issues due to its equitable relief, pleadings are complicated when the injustices do not rise to unlawful or fraudulent conduct, leaving potential litigants to instead allege "unfair" practices. "In determining whether a particular business practice is unfair under [the UCL], the court must weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim."[27] What constitutes "unfair competition" or an "unfair

22. CAL. BUS. & PROF. CODE § 17200 (1993).

23. No. 15-MD-02617, 2016 WL 3029783 (N.D. Cal. May 27, 2016).

24. *Id.* at *32 (quoting Berger v. Home Depot U.S.A., Inc., 476 F. Supp. 2d 1174, 1177 (C.D. Cal. 2007)).

25. *Id.* (quoting Rose v. Bank of Am., 304 P.3d 181, 185 (Cal. 2013)).

26. *Id.*

27. *Actions Permitted*, CAL. CIV. PRAC. BUSINESS LITIGATION § 60:5 (2026).

or fraudulent business practice" is a question of fact, with "the essential test being whether the public is likely to be deceived."[28] "[R]ules of unfair competition are based, not alone upon the protection of a property right existing in the complainants, but also upon the right of the public to protection from fraud and deceit."[29]

Even if the court determines that a certain practice is unfair, the UCL has additional procedural requirements: that is, whether the information can be considered property, and whether this property was injured in fact. Regarding the question of whether personal information is property, the court first considered the question in *Thompson v. Home Depot, Inc.*[30] In that case, the plaintiff brought an action under the UCL against Home Depot for requiring customers to fill out a preprinted form that required his personal identification "as a condition to performing a credit card transaction."[31] The personal information was neither stolen nor subject to any data breach, therefore the court held that the plaintiff's argument that his personal information constitutes property under the UCL, was "unpersuasive."[32]

The Northern District of California has drawn on other state jurisdictions, such as New York, to determine whether personal information should be considered property: "There is . . . no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large."[33] In a similar fashion, the court cited an Illinois Court of Appeals decision in which the Illinois court rejected a claim of tortious appropriation after the defendant sold credit cardholder names, reasoning that the "cardholder's name has little or no intrinsic value apart from its inclusion on a categorized list."[34]

After a plaintiff has satisfied a showing of at least one of the three prongs of the UCL, a plaintiff must then make "a twofold showing" of both injury in fact and a loss of money and/or property caused by unfair competition.[35] The California Supreme Court has stated that

---

28. People v. Toomey, 203 Cal. Rptr. 642, 652 (Ct. App. 1984) (quoting Payne v. United Cal. Bank, 100 Cal. Rptr. 672, 676 (Ct. App. 1972)).

29. People *ex rel.* Mosk v. Nat'l Rsch. Co., 20 Cal. Rptr. 516, 520–21 (Ct. App. 1962) (quoting Acad. of Motion Picture Arts & Scis. v. Benson, 104 P.2d 650, 653 (Cal. 1940)).

30. No. 07cv1058, 2007 WL 2746603 (S.D. Cal. Sep. 18, 2007).

31. *Id.* at *1.

32. *Id.* at *3.

33. *Id.* at *3 (quoting *In re* JetBlue Airways Corp. Priv. Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005)) (alteration in original).

34. *Id.* at *3 (summarizing the holding of Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995)).

35. Susilo v. Wells Fargo Bank, N.A., 796 F. Supp. 2d 1177, 1195–96 (C.D. Cal. 2011) (quoting Peterson v. Cellco P'ship, 80 Cal. Rptr. 3d 316, 321 (Ct. App. 2008)).

"[t]here are innumerable ways in which economic injury from unfair competition may be shown."[36] A plaintiff may:

> (1) surrender in a transaction more, or acquire in a transaction less, than [they] otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which [they] ha[ve] a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.[37]

However, the Northern District of California has varied in its opinion on whether claims regarding personal information demonstrate these injuries in fact.

II. APPLYING THE UCL: 2016 TO 2024

A. The Facebook *Standard Era*

In *In re Anthem, Inc. Data Breach Litigation*, the court addressed a UCL claim based on harm to personal information five years after *Facebook*. There, Anthem collected "individually identifiable health record information" and maintained it in a common database, promising plaintiffs their information would be protected through "privacy notices, online website representations, and other advertising."[38] Anthem collected the personal information and, according to the plaintiffs, Anthem and the other defendants failed to respond to safety warnings about cyberattacks, thus leading to the health information leak from the database.[39]

The plaintiffs advanced theories of unfairness, unlawfulness, and fraud—all three UCL prongs.[40] The court found that the plaintiffs had accurately represented unlawfulness, alleging violations of HIPAA and the FTC Act, among various consumer protection acts.[41] For the unfairness prong, the court stepped away from the aforementioned fact-intensive inquiry, instead stating that California courts take a

---

36. Kwikset Corp. v. Superior Ct., 246 P.3d 877, 885 (Cal. 2011).

37. *Id.* at 885–86.

38. *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617, 2016 WL 3029783, at *2 (N.D. Cal. May 27, 2016). These records included

> personal information (such as names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information, including income data) and individually-identifiable health information (pertaining to the individual claims process, medical history, diagnosis codes, payment and billing records, test records, dates of service, and all other health information that an insurance company has or needs to have to process claims).

Id.

39. *Id.* at *2–3.

40. *Id.* at *33–34.

41. *Id.* at *33.

variety of approaches.[42] Under the balancing approach, courts must "weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim."[43] Under the tethering test, "unfairness must be tethered to some legislatively declared policy or proof of some actual or threatened impact on competition."[44] Lastly, under the FTC test, "(1) the consumer injury must be substantial; (2) the injury must not be outweighed by any countervailing benefits to consumers or competition; and (3) it must be an injury that consumers themselves could not reasonably have avoided."[45] The court followed the balancing test, noting that based on the balancing test alone the plaintiffs had standing, reasoning that adjudging utility against gravity of the harm is a process inherently resolved later in litigation.[46] Notably, the court mentioned that the plaintiffs' standing was also based on the showing that each plaintiff had paid money for health insurance premiums, which were used to pay for services offered by Anthem and other defendants.[47] Therefore, the injury-in-fact requirement was satisfied by an actual loss of money or property.[48]

The next year, the court considered *In re Yahoo! Inc. Customer Data Security Breach Litigation*,[49] a multidistrict litigation in which plaintiffs who used Yahoo Mail and Yahoo Small Business were required to provide their personal information to obtain the services.[50] This data was cyberattacked, like in *In re Anthem*, though a similar prior incident had put Yahoo on notice of its privacy deficiencies.[51] The court took a different approach with the personal information provided to Yahoo, stating that while "'injury in fact' may be intangible and need not involve lost money or property . . . a UCL plaintiff's 'injury in fact' [must] specifically involve lost money or property."[52] The plaintiffs argued that their injuries included future costs of protecting their personal information from additional cyberattacks, but the court responded that "'intangible' allegations of future costs" do not show a specific loss of money or property due to

42. *Id.*

43. *Id.* (quoting Davis v. HSBC Bank Nev., N.A., 691 F.3d 1152, 1169 (9th Cir. 2012)).

44. *Id.* (quoting Lozano v. AT&T Wireless Servs., Inc., 504 F.3d 718, 735 (9th Cir. 2007)).

45. *Id.* (quoting Camacho v. Auto. Club of S. Cal., 48 Cal. Rptr. 3d 770, 777 (Ct. App. 2006)).

46. *Id.* at *34.

47. *Id.* at *30.

48. *Id.*

49. *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752, 2017 WL 3727318, at *1 (N.D. Cal. Aug. 30, 2017).

50. *Id.*

51. *Id.*

52. *Id.* at *22 (quoting Ehret v. Uber Techs., Inc., 68 F. Supp. 3d 1121, 1132 (N.D. Cal. 2014)) (alterations in original).

the defendants' misconduct.[53] However, the court noted that though the plaintiffs lacked Article III standing, they had adequately alleged a "real and immediate threat of repeated injury" from defendants and therefore had standing to seek injunctive relief under the UCL.[54]

B. The Fourth Circuit Weighs In

One year later, Marriott, the hotel and resort management company, was the target of a data breach in 2018 after a merger with Starwood, a similar entity, where hackers obtained personal information from guests which, according to the Marriott privacy statement, was not collected and saved. The hackers stole "names, mailing addresses, phone numbers, email addresses, passport numbers, . . . dates of birth, gender, . . . payment card numbers, payment card expiration dates, and tools needed to decrypt cardholder data."[55]

Those affected sued Marriott in a consolidated action, alleging that Marriott "failed to conduct appropriate due diligence of Starwood's cybersecurity risks before and after the merger, despite the fact that Starwood disclosed a data breach . . . and after knowing that it and other hotel chains were the targets of security threats in the months and years preceding the data breach."[56] Advancing all three theories of unfairness, unlawfulness, and fraud under the UCL, the California plaintiffs alleged that Marriott violated the UCL by:

> failing to implement and maintain reasonable security measures . . . , failing to comply with common law and statutory duties . . . , misrepresenting that it . . . protect[ed] the privacy . . . of Plaintiffs' personal information, and concealing the material fact that it did not reasonably secure Plaintiffs' personal information or comply with statutory duties.[57]

The Federal District Court of Maryland noted that the Fourth Circuit had not yet decided whether the loss of property value in personal data fell under the umbrella of injury for the purpose of UCL litigation but recognized that doing so was a "growing trend" in courts across the nation.[58] However, the court acknowledged that California courts are also recognizing the opposite:

> [O]ther courts have reached the exact opposite conclusion and denied motions to dismiss UCL claims in data breach cases. For

---

53. *Id.*

54. *Id.* at *31 (quoting Bates v. United Parcel Serv., Inc., 511 F.3d 974, 985 (9th Cir. 2007)).

55. *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 454 (D. Md. 2020).

56. *Id.*

57. *Id.* at 490–91.

58. *Id.* at 460–61.

> example, in *In re Anthem, Inc. Data Breach Litigation*, Judge Koh found that the plaintiffs' allegations that they lost the benefit of their bargain was sufficient to satisfy the economic injury requirement for standing under the UCL, explaining that this type of loss "mirrors the California Supreme Court's determination in *Kwikset* that a plaintiff who has 'surrender[ed]in a transaction more, or acquire[d] in a transaction less, than he or she otherwise would have' may bring a UCL claim."[59]

The Northern District of California seemingly agreed with the *Marriott* court's reasoning in 2021's *Calhoun v. Google LLC*.[60] In *Calhoun*, the plaintiffs were Google users who took advantage of the opportunity to not "sync" their Chrome browsers with their Google accounts, a feature which typically enables Chrome to store personal information.[61] The plaintiffs alleged that Chrome actually does send information to Google whenever "a user exchanges communications with any website that includes Google surveillance source code . . . regardless of whether a user is logged-in to Google Sync or not."[62]

In an interesting change of opinion, the court rejected Google's argument that the plaintiffs lacked standing under the UCL without alleging any loss of money or property,[63] instead stating that "to satisfy the statutory standing requirement under the UCL, a plaintiff must merely suffer an injury in fact that is an 'economic injury.'"[64] The court concluded that the Google plaintiffs had met this requirement, saying, "[i]ndeed, the Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing."[65]

Google was sued again under the UCL in 2024's *A.B. ex rel. Turner v. Google LLC*,[66] when a group of six underage plaintiffs alleged that Google violated their privacy by collecting their personal information without parental consent through its many integrated applications.[67] Google responded that the plaintiffs had no UCL standing because they did not allege an economic injury.[68] According to Google, the "misappropriation of personal information" does (and

---

59. *Id.* at 492 (quoting *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016)).

60. 526 F. Supp. 3d 605 (N.D. Cal. 2021).

61. *Id.* at 613.

62. *Id.* (alteration in original).

63. *Id.* at 636.

64. *Id.* (quoting Kwikset Corp. v. Superior Ct., 246 P.3d 877, 885 (Cal. 2011)).

65. *Id.*

66. 737 F. Supp. 3d 869 (N.D. Cal. 2024).

67. *Id.* at 874.

68. *Id.* at 881.

effectively should) not give rise to injury under current California law.[69]

However, the court acknowledged that there was a split of opinion in the District and Ninth Circuit precedent.[70] It ultimately agreed with *Calhoun* and *Brown*, concluding that the plaintiffs had adequately pled the economic injury needed to establish UCL standing.[71] It stated, "[p]rivacy harms involving personal data can constitute an injury to money or property sufficient to provide standing under the UCL,"[72] and the "plaintiffs here recognize that there is a market for their data, alleging in their complaint that 'there is a market for consumers to monetize Personal Information and the behavioral preferences that Defendants have usurped.'"[73]

III. STRATEGIC PLEADINGS UNDER THE UCL

How the *Calhoun*, *Brown*, and *A.B.* courts managed to come to their conclusions may be answered by taking a closer look at the litigants' pleadings. The plaintiffs in *A.B. v. Google* raised the "market for consumers" argument,[74] but looking back to *Facebook*, those plaintiffs neither alleged monetary damages nor that they paid for Facebook's services.[75] Instead, the plaintiffs alleged that Facebook "unlawfully shared their 'personally identifiable information' with third-party advertisers," and the court immediately dismissed the claim on the basis that "'personal information' does not constitute property under the UCL,"[76] and "[b]ecause Plaintiffs allege that they

69. *Id.* (first citing Pruchnicki v. Envision Healthcare Corp., 845 F. App'x 613, 615 (9th Cir. 2021) (holding that "'mere misappropriation of personal information' does not establish compensable damages"); and then citing *In re* Google, Inc. Priv. Pol'y Litig., No. 12-cv-001382, 2015 WL 4317479, at *5 n.63 (N.D. Cal. July 15, 2015) (finding the misappropriation of personal information without a resultant economic harm to be neither damage nor injury in fact)).

70. *Id. Compare In re* Facebook Priv. Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011), *aff'd* 572 F. App'x 494 (9th Cir. 2014) ("[P]ersonal information does not constitute property for purposes of a UCL claim."), *with Calhoun*, 526 F. Supp. 3d at 636 (concluding that "plaintiffs who suffered a loss of their personal information suffered economic injury and had standing"), *and* Brown v. Google LLC, No. 20-CV-03664, 2021 WL 6064009, at *15 (N.D. Cal. Dec. 22, 2021) (finding the loss of personal information through Google's data collection as sufficient to qualify as the diminution of a future property interest).

71. *A.B.*, 737 F. Supp. 3d at 881.

72. *Id.* (quoting *In re* Meta Pixel Tax Filing Cases, 724 F. Supp. 3d 987, 1024 (N.D. Cal. Mar. 25, 2024) (showing that privacy harms constitute economic injury for UCL standing in three instances: unfair benefit-of-the-bargain to businesses, diminished value, and reduced right to exclude)).

73. *Id.* at 881.

74. *Id.*

75. *Facebook*, 791 F. Supp. 2d at 714.

76. *Id.*

received Defendant's services for free, as a matter of law, Plaintiffs cannot state a UCL claim under their own allegations."[77]

In *Brown*, the plaintiffs also did not pay for Google services, but they advanced a theory of economic harm by claiming that they suffered injury-in-fact "as a result of . . . the unauthorized disclosure and taking of their personal information which *has value* as demonstrated by its use and sale by Google."[78] "Specifically, Plaintiffs 'have suffered harm in the form of diminution of the value of their private and personally identifiable data and content.'"[79] The court explained:

> These detailed allegations establish at least two cognizable theories of economic injury. First, because Google previously has paid individuals for browsing histories, it is plausible that, had Plaintiffs been aware of Google's data collection, they would have demanded payment for their data. Thus, by inducing Plaintiffs to give Google their data without payment, Google caused Plaintiffs to "acquire in a transaction less[] than [they] otherwise would have." Second, because there are several browsers and platforms willing to pay individuals for data, it is plausible that Plaintiffs will decide to sell their data at some point.[80]

The court found that Google's argument entirely ignored the California Supreme Court's ruling that a UCL claim "may be based on any kind of 'economic injury.'"[81] Therefore, the plaintiffs "plausibly alleged" that Google's conduct caused Plaintiffs to have a "'diminished' . . . 'future property interest,'" and the injuries stood "well within" the categories already recognized by the court.[82]

The differences in finding injury in fact may stem from differences in pleading the claim. The Federal Rules of Civil Procedure outline that under Rule 8(a) pleading must contain a "short and plain statement of the claim showing that the pleader is entitled to relief."[83] Historically, such pleadings were "notice pleadings," meaning that the case could not be dismissed for failure to state a claim upon which relief could be granted under Rule 12(b)(6) unless

77. *Id.* at 715.

78. Brown v. Google LLC, No. 20-CV-03664, 2021 WL 6064009, at *14 (N.D. Cal. Dec. 22, 2021) (alteration in original) (emphasis added) (quoting Plaintiffs' Second Amended Complaint at ¶ 282, *Brown*. 2021 WL 6064009 (No. 136-1)).

79. *Id.* (quoting Plaintiffs' Second Amended Complaint at ¶¶ 279, 281, *Brown*, 2021 WL 6064009 (No. 136-1)).

80. *Id.* at *15 (alteration in original) (citation omitted) (quoting Kwikset Corp. v. Superior Ct., 246 P.3d 310, 324 (Cal. 2011).

81. *Id.* at *16.

82. *Id.* (quoting *Kwikset*, 246 P.3d at 885–86).

83. FED. R. CIV. P. 8(a)(2).

"it appear[ed] beyond doubt that the plaintiff [could] prove no set of facts in support of his claim which would entitle him to relief."[84]

In 2007, the Supreme Court put an end to notice pleading in *Bell Atlantic Corporation v. Twombly*.[85] The Court stated that Rule 8(a) requires plaintiffs in antitrust litigation to plead "enough facts to state a claim to relief that is plausible on its face."[86] Giving lower courts some guidance, the Supreme Court clarified that the pleading standard does not require "detailed factual allegations," but still demands more than an "unadorned . . . accusation."[87] Additionally, a "formulaic recitation of the elements of a cause of action will not do."[88] Instead, the complaint must demonstrate enough facial plausibility for the court to draw a reasonable inference that the defendant could be liable for the alleged offense.[89] Later, in 2009, the Court clarified in *Ashcroft v. Iqbal*[90] that the heightened Rule 8(a) pleading standard governs "all civil actions and proceedings in the United States district courts," not just antitrust actions.[91]

The Northern District of California follows federal pleading standards and applies them to UCL claims, but still *Facebook* was filed and decided after the *Twombly-Iqbal* decisions changed pleadings requirements from notice pleading to particularized facts that could sustain a claim.[92] However, researchers Mark Anderson and Max Huffman note that during the early 2010s, "'thanks to' *Twombly* and *Iqbal*, 'federal pleading standards [were] in a crisis.'"[93] A lack of subsequent caselaw immediately post-*Twombly-Iqbal* made it difficult for potential plaintiffs to plead their claims in a manner that would avoid dismissal. Additionally, the guidance upon which federal courts followed the Supreme Court is that *Twombly-Iqbal* pleading standards created the "unifying rationale that avoidance of litigation per se—independent of any resulting liability—is a sufficiently worthy goal to restrict court access to plaintiffs,"[94]

84. Conley v. Gibson, 355 U.S. 41, 45–46 (1957).

85. 550 U.S. 544 (2007).

86. *Id.* at 570.

87. *Id.* at 555; Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 555).

88. *Twombly*, 550 U.S. at 555.

89. *Id.* at 556; *see Iqbal*, 556 U.S. at 679.

90. 556 U.S. 662, 678 (2009).

91. *Id.* at 684 (quoting FED. R. CIV. P. 1).

92. *See generally* Douglas G. Smith, *The Evolution of a New Pleading Standard:* Ashcroft v. Iqbal, 88 OR. L. REV. 1053 (2009) (explaining how the federal notice pleading standard changed in the early 2000s).

93. Mark Anderson & Max Huffman, Abstract, Iqbal*,* Twombly*, and the Expected Cost of False Positive Error*, 20 CORN. J.L. & PUB. POL'Y 1, 1 (2010) (quoting Adam N. Steinman, *The Pleading Problem*, 62 STAN. L. REV. 1293, 1295 (2010)).

94. *Id.* at 18.

meaning federal courts used this standard to dismiss claims more easily.

UCL plaintiffs may have very well been among those struggling in the wake of *Twombly-Iqbal*. The timeline of data privacy caselaw presented here indicates a more concentrated dismissal of claims over the lack of particularized facts within the complaint, such as detailed allegations demonstrating injury in fact, immediately post-*Twombly-Iqbal* as compared to present day. Though the possibility remains that UCL plaintiffs have simply learned how to more artfully plead their injuries in fact to prevent dismissal of the complaint under Rule 12(b)(6), perhaps the change is more accurately captured by changes in California state law and local attitudes towards big tech and data privacy.

IV. A NEW SERIES OF LEGISLATION

The *Calhoun* decision noted that the data in question "falls within the definition of personal information under California law, which governs Google's Terms of Service."[95] It cited California law definitions, where personal information is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including "[i]nternet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement."[96] However, these laws and definitions come from the California Consumer and Privacy Act of 2018 (the CCPA), not the UPL.

The CCPA was passed in 2018 (effective in 2020) after two California natives were the subject of identity theft and data fraud.[97] With community support and a shared passion of keeping control of their data, they introduced a measure on the ballot for statewide approval, and it passed.[98] The CCPA aims to secure privacy rights in California, including the right to know about the personal information collected, the right to delete any information collected, and the right to limit the use and disclosure of information collected.[99]

---

95. Calhoun v. Google LLC, 526 F. Supp. 3d 605, 622 (N.D. Cal. 2021).

96. CAL. CIV. CODE § 1798.140(v) (2026).

97. DeAndrea Salvador, *The Story of the CCPA*, DATAGRAIL (Aug. 9, 2021), https://perma.cc/DX36-JNYJ.

98. *Id.*

99. *California Consumer Privacy Act (CCPA)*, STATE CAL. DEP'T JUST., OFF. ATT'Y GEN. (Mar. 13, 2024), https://perma.cc/SMJ8-ZJ4H. The 2018 CCPA rights included (a) "the right to know about the personal information a business collects about them and how it is used and shared;" (b) "the right to delete personal information collected from them (with some exceptions);" (c) "the right to opt-out of the sale or sharing of their personal information;" and (d) "the right to non-discrimination for exercising their CCPA rights." *Id.*

The CCPA further places certain responsibilities on businesses, such as informing consumers about the categories of personal information collected and whether the information is sold or shared,[100] informing consumers about the retention period for personal information,[101] ensuring the collection, use, retention, and sharing of personal information are reasonably necessary and proportionate to the disclosed purposes,[102] and implementing reasonable security procedures and practices to protect personal information.[103]

The state immediately sought to amend the CCPA to keep up with the ever-changing landscape of data privacy concerns.[104] Voters passed Proposition 24, the California Privacy Rights Act of 2020 (the CPRA), which included additional privacy protections for the CCPA, such as permitting consumers to: "(1) prevent businesses from sharing personal information; (2) correct inaccurate personal information; and (3) limit businesses' use of 'sensitive personal information'—including precise geolocation; race; ethnicity; religion; genetic data; private communications; sexual orientation; and specified health information."[105] Additionally, the proposition established the California Privacy Protection Agency (the Agency) to implement and enforce the CCPA.[106]

Regardless of the initial CPRA amendments, like the UCL, the CCPA lacks any teeth to significantly effect change regarding unfair practices with privacy. According to the statutory scheme, any allegations of violations of the CCPA begin first with an investigation by the Agency.[107] The Agency has complete discretion over the allegations and may choose to not act on any certain matter.[108] If the Agency does, however, choose to engage with the complaint, whoever brought the allegation of a violation must follow a bureaucratic process with first notice of violation being sent to the alleged violator followed by a hearing on violation.[109] If the Agency determines there has been a violation, it shall issue an order that may require the

100. CAL. CIV. CODE § 1798.100(a)(1)–(2) (2025).

101. *Id.* § 1798.100(a)(3).

102. *Id.* § 1798.100(c).

103. *Id.* § 1798.100(e).

104. California Privacy Rights Act of 2020, 2020 Cal. Stat. A-84, A-88 (codified as amended at CAL. CIV. CODE §§ 1798.100–.199.100).

105. OFFICIAL VOTER INFORMATION GUIDE: CALIFORNIA GENERAL ELECTION TUESDAY, NOVEMBER 3, 2020, CAL. SEC'Y OF STATE (2020), https://perma.cc/JWY3-T9FL. *See also* California Privacy Rights Act of 2020, 2020 Cal. Stat. A-90, A-91, A-93, A-105, A-106 (codified as amended at CAL. CIV. CODE §§ 1798.105, .106, .121, .140); Sara Morrison, *California Just Strengthened Its Digital Privacy Protections Even More*, VOX (Nov. 4, 2020), https://perma.cc/G8NS-2YUZ.

106. *See* Morrison, *supra* note 105.

107. CAL. CIV. CODE § 1798.199.45 (2026).

108. *Id.* § 1798.199.45(b)(i).

109. *Id.* §§ 1798.199.50, .55.

violator to cease and desist violation of this title and pay an administrative fine.[110]

The CCPA is a valuable starting point for protection of personal information, but it leaves significant room for improvement. The Act cannot affect equitable relief as meaningful as the UCL can and leaves potential plaintiffs at the whims of the California Privacy Protection Agency, its discretion, and its limited injunctive power. If either (or any interested) party is unsatisfied with the Agency's decision, the statute provides for a request for judicial review to be adjudicated by an abuse of discretion standard, effectively always siding with the Agency, save for plain error.[111] Furthermore, if the Attorney General wishes to pursue investigation or civil action against a potential violator, the Agency must stay all investigations of its own, leaving it powerless to help those injured in data breach actions.[112]

V. REMEDYING THE STATUTORY DEFICIENCIES

A. The UCL

If both the UCL and the CCPA fail to address potential plaintiffs, how can the laws adapt? As for the UCL, a rebuttable presumption of injury in fact would reconcile the Northern District's many different findings of injury in fact and emphasize that the law serves to aid not just those who correctly pled their case but also to all who fear their private information has been the victim of unfair, unlawful, or fraudulent business practices.

Under California state law, "A presumption is either conclusive or rebuttable. Every rebuttable presumption is either (a) a presumption affecting the burden of producing evidence or (b) a presumption affecting the burden of proof."[113] As mentioned by legal scholar Francis H. Bohlen, "[t]he need of relaxing the stringency of the proof in theory required by the common law has led courts to create certain presumptions."[114] One such presumption arises "[w]hen the power to produce evidence of the fact on which the litigant's rights depend is exclusively in the power of the opponent of

110. *Id.* § 1798.199.55. Specifically, the violator must "(1) Cease and desist violation of this title [and] (2) Subject to [s]ection 1798.155, pay an administrative fine of up to two thousand five hundred dollars ($2,500) for each violation, or up to seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers. When the agency determines that no violation has occurred, it shall publish a declaration so stating." *Id.* § 1798.199.55(a).

111. *Id.* § 1798.199.85.

112. *Id.* § 1798.199.90(c).

113. CAL. EVID. CODE § 601 (2026).

114. Francis H. Bohlen, *The Effect of Rebuttable Presumptions of Law Upon the Burden of Proof*, 68 U. PA. L. REV. 307, 314 (1920).

him, who, having the risk of persuasion, should in theory also bear the burden of producing evidence sufficient to persuade."[115]

The UCL plaintiffs would still have to satisfy the burden of production, that is, evidence demonstrating a harm to personal information, but, if satisfied, the burden of proof would be shifted to the defendants, who would have to disprove the injury in fact. Companies such as Google or Meta have better access to data markets and quantifiable numbers regarding the value of personal information, so not only would shifting the burden of proof allow plaintiffs a better opportunity at going forward with their claims, but also less time and money will be spent in the discovery process, allowing plaintiffs to pursue claims that they may not have had the wherewithal to pursue.

Additionally, in the age of developments in artificial intelligence, internet users and potential plaintiffs are even more concerned about internet privacy and the protection of their personal information,[116] and therefore the rationale for developing the rebuttable presumption is even stronger. The Pew Research Center found in 2023 that although 90% of Americans have heard "at least a little about AI," around 52% of Americans felt more *concerned* than *excited* about AI use in daily life.[117] When questioned about AI implementation in more personal areas, such as employers using AI to analyze employees' facial expressions or heath care providers relying on AI for their medical care, respectively 70% and 60% of respondents opposed these utilizations.[118] Implementing the rebuttable presumption as a procedural safeguard can alleviate concerns that the average internet user may harbor, for they would be equipped with the knowledge that businesses would carry the burden of disproving unfair practices with their personal information.

B. The CCPA

As for the CCPA, amending the statute to provide a private right of action under tort law would allow those injured to act when their personal information has been violated, without having to first exhaust the administrative system or be subject to the whims of the Attorney General. The CCPA already creates minimum duty standards for businesses, and plaintiffs can then demonstrate breach, causation, and injury, and can be awarded damages commensurate with the harm suffered. Though these damages may be small, lending to the establishment of class action litigations to sue, the court may

115. *Id.*

116. Michelle Faverio & Alec Tyson, *What the Data Says About Americans' Views of Artificial Intelligence*, PEW RSCH. CTR. (Nov. 21, 2023), https://perma.cc/XCF2-NJBK.

117. *Id.*

118. *Id.*

also be able to award equitable remedies not currently available to a private individual. These remedies can include requirements that the company warn the public of its data breaches and sales, implementations of the proper safeguards are in place to prevent data collection of those who do not wish to "opt-in" to collection, or increased disclosures of data use to promote greater company transparency about how personal information is stored and used. Therefore, instead of empowering the Agency and the Attorney General to enforce the CCPA, those who wish to utilize the statute can take ownership over their allegations of violation, and thus, over their personal information.

VI. THE FUTURE OF INTERNET PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Concerns about AI are dominating the conversation around data privacy and protection of personal information. Personal information—data—is the "fundamental basis for the functionality and advancement of AI."[119] "AI systems demand access to comprehensive personal datasets" in order to develop, gain knowledge, and adjust accordingly.[120] The biggest concern about these systems regarding data privacy is that the gathering and use of personal information "frequently take[s] place without explicit consent or understanding of [those] involved."[121]

Additionally, these systems are rapidly advancing, making the definition and regulation of AI difficult, especially in the legal system, which "struggle[s] to keep peace with the fast pace of technological advancements, leaving gaps in accountability and liability."[122] California is already anticipating reform and has published draft regulations under the CCPA regarding risk assessments. The draft would create a business duty to complete a risk assessment that is automatically triggered when a business processes California residents' personal information to train Generative AI technologies, meaning that automatically engaging in such activities presents significant risks to privacy.[123]

California Governor Gavin Newsom signed Assembly Bill 1008 into law on August 30, 2024, expanding the definition of personal information under the CPRA to include AI models, imposing

119. Prajeet Sen, *Balancing Act: Navigating Artificial Intelligence, Data Privacy, and Legal Challenges in the Digital Age*, 7 INT'L J.L. MGMT. & HUMS. 3062, 3065 (2024).

120. *Id.*

121. *Id.*

122. Ashish Chaturvedi, *Defining Legal Responsibility in the Age of AI: Addressing Gaps in Data Privacy Regulation*, 3 INDIAN J. INTEGRATED RSCH. L. 1, 3 (2023).

123. Jonathan Tam, *Privacy Law Issues Associated with Developing and Deploying Generative AI Tools*, 1 CAL. LAW. ASSOC. PRIV. L.J. 5, 6 (2024).

requirements on businesses using AI, and broadening privacy protections to data utilized by Generative AI.[124] Additionally, Governor Newsom signed Assembly Bill 2013 into law, requiring developers of AI systems or services to "post on the developer's internet website documentation regarding the data used by the developer to train the generative artificial intelligence system or service,"[125] thus furthering consumer understanding and government regulation of rapidly-developing AI.

More recently, Governor Newsom approved the California AI Transparency Act (CAITA) to go into effect January 1, 2026.[126] Under the statutory scheme, the CAITA would require "covered providers," that is, "a person that creates, codes, or otherwise produces a generative artificial intelligence system that has over 1,000,000 monthly visitors or users and is publicly accessible within the geographic boundaries of the state,"[127] to "make available an AI detection tool at no cost to the user" that meets criteria such as allowing a user to "assess whether image, video, or audio content, or content that is any combination thereof, was created or altered by the covered provider's [generative AI] system."[128] Additionally, the

---

124. Anas Baig et al., *AB 1008: California's Move to Regulate AI and Personal Data*, SECURITI (Feb. 25, 2025), https://perma.cc/M2DH-BTC4.

125. CAL CIV. CODE § 3111 (2026).

126. California AI Transparency Act, CAL. BUS. & PROF. CODE §§ 22757–22757.6 (operative Aug. 2, 2026); *see also* 2025 Governor's Signing Message, Assem. Bill No. 853 (2025–2026 Reg. Session.), *reprinted in* Cal. Assem. J. 3475 (daily ed.).

127. CAL. BUS. & PROF. CODE § 22757.1 (operative Aug. 2, 2026).

128. CAL. BUS. & PROF. CODE § 22757.2 (operative Aug. 2, 2026). The AI detection criteria include:

> (1) The tool allows a user to assess whether image, video, or audio content, or content that is any combination thereof, was created or altered by the covered provider's GenAI system.
> (2) The tool outputs any system provenance data that is detected in the content.
> (3) The tool does not output any personal provenance data that is detected in the content.
> (4) (A) Subject to subparagraph (B), the tool is publicly accessible.
> (B) A covered provider may impose reasonable limitations on access to the tool to prevent, or respond to, demonstrable risks to the security or integrity of its GenAI system.
> (5) The tool allows a user to upload content or provide a uniform resource locator (URL) linking to online content.
> (6) The tool supports an application programming interface that allows a user to invoke the tool without visiting the covered provider's internet website.

Id. The statutory scheme further provides:

> (b) A covered provider shall collect user feedback related to the efficacy of the covered provider's AI detection tool and incorporate relevant feedback into any attempt to improve the efficacy of the tool.

covered providers shall not "collect or retain personal information from users of the covered provider's AI detection tool" unless the user opts in submitting feedback for the development and improved efficacy of the tool.[129] Those covered providers who violate the statute are to be subject to a civil penalty of $5,000 per violation "to be collected in an action brought by the Attorney General, a city attorney, or a city council."[130]

The ever-changing attitudes towards AI, along with its nature, demand a "flexible and adaptable approach to legal regulation."[131] The advances in California with the CCPA, CPRA, and CAITA all evidence notable improvements in this regard. However, as Prajeet Sen notes, "their efficacy in dealing with the swift progress of AI technologies necessitates continual assessment and adjustment."[132] Not only do regulations for privacy protection require constant upkeep, but they require new schemes of liability: "[I]t is necessary to demarcate the lines of responsibility for AI systems. This could involve implementing a system of liability that allocates responsibility to those who design, develop, and deploy AI systems."[133] The CAITA takes important first steps to better regulate AI so as to protect internet consumers. However, to best protect internet users from privacy violations coming from the use of artificial intelligence, regulatory schemes need to create new legal definitions, classes of violations, and schemes of liability and crack down when violations occur.

CONCLUSION

If the UCL or CCPA are not remedied, future potential plaintiffs will continue to feel the impact the statutes' inadequacies. As Joseph

---

> (c) A covered provider shall not do any of the following:
> (1) (A) Except as provided in subparagraph (B), collect or retain personal information from users of the covered provider's AI detection tool.
> (B) (i) A covered provider may collect and retain the contact information of a user who submits feedback pursuant to subdivision (b) if the user opts in to being contacted by the covered provider.
> (ii) User information collected pursuant to clause (i) shall be used only to evaluate and improve the efficacy of the covered provider's AI detection tool.
> (2) Retain any content submitted to the AI detection tool for longer than is necessary to comply with this section.
> (3) Retain any personal provenance data from content submitted to the AI detection tool by a user.

Id.

129. *Id.* § 22757.2(c)(1)(A).
130. *Id.* § 22757.4(a).
131. Sen, *supra* note 119, at 3068.
132. *Id.*
133. Chaturvedi, *supra* note 122, at 4.

W. Jerome notes in *Buying and Selling Privacy*, "[b]ig data is transforming individual privacy—and not in equal ways for all. We are increasingly dependent upon technologies, which in turn need our personal information in order to function. This reciprocal relationship has made it incredibly difficult for individuals to make informed decisions about what to keep private."[134] Furthermore, the price an individual assigns to their personal information is subjective, and a lack of transparency around the value of data causes many to suffer difficulties in protecting their personal information.[135]

Specifically, "[w]hile the benefits of the data economy will accrue across society, the wealthy, better educated are in a better position to become the type of sophisticated consumer that can take advantage of big data," meaning those in the lower class are "likely to feel the biggest negative impact from big data."[136] Jerome concludes:

> Big data worsens this problem. Most of the biggest concerns we have about big data—discrimination, profiling, tracking, exclusion—threaten the self-determination and personal autonomy of the poor more than any other class. Even assuming they can be informed about the value of their privacy, the poor are not in a position to pay for their privacy or to value it over a pricing discount, even if this places them into an ill-favored category.[137]

Clearly, California is responding to its residents' fears over data security and protection of personal information, but the primary statutes under which litigants can make a claim fail to meaningfully address their concerns and come up short. The UCL places an intense burden on claimants, a burden that has the potential to monetarily deter future litigation due to the high costs of discovery. The CCPA requires bureaucratic exhaustion before a violated consumer can request Attorney General intervention, which is still a discretionary action. The CAITA allows for some consumer protections against AI collecting and utilizing personal data, but with some AI companies fetching valuations of up to $30 billion,[138] a $5,000 per violation fine neither will have a likely or substantial deterring effect on covered

134. Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, 47 (2013).

135. *Id.* at 48.

136. *Id.* at 50.

137. *Id.* at 51.

138. *See, e.g.*, Chris Cannon, *Startup Trends: These "Big 3" AI Companies Reach Their Highest Valuations Yet*, FORGE (Dec. 1, 2025), https://forgeglobal.com/insights/startup-trends-these-big-3-ai-companies-reach-their-highest-valuation-yet/ (estimating OpenAI has a valuation of $500 billion, Anthropic of $350 billion, and xAI of $130.15 billion); Kate Clark, *OpenAI Co-Founder Sutskever's Startup is Fundraising at $30 Billion-Plus Valuation*, BLOOMBERG (Feb. 17, 2025), https://www.bloomberg.com/news/articles/2025-02-17/openai-co-founder-s-startup-is-fundraising-at-a-30-billion-plus-valuation.

providers nor assure internet consumers of the safety of their personal information.

Especially in the age of artificial intelligence, consumers, more than ever, are concerned about the use and collection of their personal information. While the UCL, CCPA, and CAITA make tremendous strides towards protecting consumer interests from predatory internet practices, California needs to continue protecting all internet users by implementing ongoing reforms that incentivize more litigation, thereby increasing business transparency and allowing for easier regulation of both current and forthcoming data collection methods. Only with a large swath of statutory protections will the inequities of big data be resolved, and those who make uninformed decisions about their data—to the benefit of large technology companies with greater bargaining power—will finally be in a better position to control (and potentially litigate the use of) their personal information.

Emily Mundt[*]

[*] J.D., 2026, Wake Forest University School of Law; B.S.F.S. International History, 2023, Georgetown University. Thank you to Will Boyce, Andrew Harp, Grace Mohlin, and the rest of the Wake Forest Law Review for their support in making this Comment publishable. Thank you also to my family, friends, and loved ones for encouraging me throughout these last three years—everything I do contains a piece of you.