Journal of Business & Technology Law

Volume 17 | Issue 1 Article 5

Facebook's "Like" Button Plugin and User Tracking: Stretching Outdated and Ambiguous Laws to Protect User Privacy

David Brokaw

Facebook's "Like" Button Plugin and User Tracking: Stretching Outdated and Ambiguous Laws to Protect User Privacy

DAVID BROKAW*©

ABSTRACT

With its 2020 decision in *Davis v. Facebook, Inc. (In re Internet Tracking Litigation*),[1] the Federal Court of Appeals for the Ninth Circuit addressed the social media site's ability to track its logged-out users' internet history using browser "cookies."[2] Browser cookies are small bits of data that are transmitted between internet users and a website and in *Davis*, these cookies were sent to Facebook when the users accessed any website that had a Facebook browser extension "plugin," even when the users were logged out of Facebook.[3]

The data sent in those browser cookies gave Facebook unauthorized access to information about the internet history of its users.[4] Facebook was able to match this information to user profiles and sold this user information to advertisers for a profit.[5] In *Davis*, the Ninth Circuit held that the putative plaintiff class had standing to sue Facebook for unjustly profiting from the unauthorized use of their data, even if they did not show any actual economic injury.[6] Also, the Ninth Circuit endorsed one position in a circuit split, finding that the unauthorized tracking of user internet

* David Brokaw was a student at the University of Maryland Francis King Carey School of Law and an Editor for the Journal of Business and Technology Law. David passed away during the summer of 2021, following his second year of law school, and is survived by his parents, Peter and Laura Brokaw. This Case Note is being published in David's honor and in recognition of his contributions to both the Journal and Maryland Carey Law community.

1. 956 F.3d 589 (9th Cir. 2020).
2. *Id.* at 595-96.
3. *Id.* at 596.
4. *Id.* at 596, 601.
5. *Id.*
6. *Id.* at 599.

usage with browser cookies, as Facebook was doing, could violate the Federal Wiretap Act.[7]

By recognizing that the unauthorized use of user internet data can give plaintiffs standing for economic claims and can implicate the Federal Wiretap Act,[8] the Ninth Circuit's decision in *Davis* could have broad ramifications on websites' liability for using cookies or internet plugins.[9] This note will begin with the factual background and procedural history of *Davis*, including a description of the technology Facebook used to track the internet usage of its users.[10] Then, this note will set forth the Ninth Circuit's analysis of the key issues raised by the plaintiff class on appeal, including whether they had standing to bring their claims, and whether they sufficiently pleaded their claims against Facebook for invasion of privacy, breach of contract, and violation of the Federal Wiretap Act.[11] Finally, this note will discuss the legal impact of the decision in *Davis* and how it may affect future litigation over the unauthorized use of user data by websites and social media companies.[12]

I. THE CASE

"On April 22, 2010, Facebook launched [its] "Like" button [social plugin on websites] outside of the Facebook domain."[13] An internet "plugin" is a program that extends the functionality of an internet browser or other internet service.[14] Facebook's "Like" button as well as other plugins extend the functionality of websites on the internet by allowing users who click the plugin to not only share content to Facebook from outside the Facebook website and indicate a "like" for products posted to Facebook, but to also allow Facebook to track users visits to these other websites with the Facebook widgets and plug-ins.[15] The "Like" button plugin was launched as part of Facebook's "Open Graph" initiative, which was an

7. *Id.* at 608 (noting that a court following the First and Seventh Circuit Courts would adopt an "understanding that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception[,]" while a court following the Third Circuit would adopt an understanding that defendant website companies "were 'the intended recipients' of . . . duplicated GET requests, and thus '[party] to [disputed] transmissions[.]'").

8. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

9. *See infra* Section III.

10. *See infra* Section I.

11. *See infra* Section II.

12. *See infra* Section III.

13. Brief for Plaintiffs-Appellants at 2, Davis v. Facebook, Inc. (*In re* Internet Tracking Litig.), 956 F.3d 589 (9th Cir. 2020) (No. 17-17486).

14. Davis v. Facebook, Inc. (*In re* Internet Tracking Litig.), 956 F.3d 589, 596 n.1 (9th Cir. 2020).

15. Bill Goodwin & Sebastian Klovig Skelton, *Facebook's Privacy Game – How Zuckerbuerg Backtracked on Promises to Protect Personal Data*, COMPUTERWEEKLY.COM (July 1, 2019), https://www.computerweekly.com/feature/Facebooks-privacy-U-turn-how-Zuckerberg-backtracked-on-promises-to-protect-personal-data.

effort by Facebook to connect the social media service with other, outside websites, envisioning a future where users could browse the web using their real identities and "everything [can] be more personalized."[16]

During the 24-hour period after Facebook launched the "Like" button, over one billion internet users encountered the plugin online.[17] By the end of April 2010, over 50,000 websites featured the "Like" button plugin, and that September Facebook announced that over 2 million different websites were using its' plugin.[18] The reach and ubiquity of the "Like" button plugin has only continued to grow, and less than a decade later, in 2018, Facebook claimed the "Like" button plugin appeared on over 8.4 million different websites.[19]

Browser cookies are simple text files shared between user web browsers and the websites they use which contain unique user identification information and share that information with the website.[20] When Facebook users visit the Facebook website, Facebook allegedly creates cookies on its users' browsers.[21] Those cookies store their user login ID information and then are able to collect the "referer headers" from the web pages visited by users.[22] A referer header request is a piece of data passed between web browsers and websites which contains the web address of the last page a user visited.[23] These referer headers can be used to track user internet usage and reveal other sensitive data.[24]

16. Caroline McCarthy, *Facebook F8: One Graph to Rule Them All*, CNET (Apr. 21, 2010, 10:25 AM), https://www.cnet.com/news/facebook-f8-one-graph-to-rule-them-all/.

17. Jason Kincaid, *5,000 Websites Have Already Integrated Facebook's New Social Plugins*, TECHCRUNCH (Apr. 29, 2010, 3:44 PM), https://techcrunch.com/2010/04/28/50000-websites-have-already-integrated-facebooks-new-social-plugins/.

18. *Id*; Leena Rao, *Five Months In, 2 Million Websites Using Facebook's New Social Plugins*, TECHCRUNCH (Sep. 30, 2010, 12:44 AM), https://techcrunch.com/2010/09/29/five-months-in-2-million-websites-using-facebooks-new-social-plugins/.

19. Letter from Rebecca Stimson, Head of Pub. Pol'y, Facebook U.K., to Damian Collins, Digit., Culture, Media and Sport Comm. Chair, U.K. House of Commons (May 14, 2018), https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/180514-Rebecca-Stimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf.

20. *What Are Cookies?* BBC: WEBWISE (Oct. 10, 2012), http://www.bbc.co.uk/webwise/guides/about-cookies.

21. Davis v. Facebook, Inc. (*In re* Internet Tracking Litig.), 956 F.3d 589, 596 (9th Cir. 2020).

22. *Id.*

23. Jennifer Kyrnin, *How to Use the HTTP Referer*, LIFEWIRE, https://www.lifewire.com/how-to-use-http-referer-3471200 (updated Jan. 16, 2020); *See also HTTP Headers*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers (modified Oct. 27, 2020) (providing background on how HTTP headers are coded).

24. *Referer Header: Privacy and Security Concerns*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns (modified July 22, 2020).

Facebook's "Like" Button Plugin and User Tracking

After the introduction of the "Like" button plugin, some noticed the plugin's ability to track user internet usage, and privacy concerns quickly arose.[25] Users were concerned about Facebook's ability to track them on websites other than Facebook with the "Like" button, even when those users did not interact with the plugin.[26] Facebook's data collection went even further: in September of 2011, an article was published on a technology blog showing that Facebook was using browser "cookies" associated with the Facebook "Like" plugin to collect data from Facebook users which included those users' personal information, even when those users were logged out of Facebook.[27] The information collected by Facebook's cookies included users' referer headers, showing their browsing history, along with those users' account identification numbers, effectively allowing Facebook to track its users across the internet.[28]

Facebook's tracking of its users' internet usage through the "Like" button plugin gave rise to legal action, including a lawsuit brought against Facebook by the Federal Trade Commission (FTC).[29] Facebook users also pursued litigation against Facebook, filing lawsuits against Facebook in various federal courts that were then consolidated into a class action suit against Facebook in the Northern District of California.[30] The consolidated suit alleged that Facebook knowingly tracked its users, even when those users were logged out of Facebook, and that the data Facebook collected from its users was valuable and marketable.[31]

Plaintiffs in the litigation represent a putative class of Facebook users with active accounts between May 27, 2010, and September 26, 2011, a time period during which they alleged that Facebook tracked its logged-out users' internet activity.[32] The plaintiff class filed their first complaint and presented several claims against Facebook, including violation of the Electronic Communications Protections Act ("Wiretap Act"), violation of the Stored Communications Act ("SCA"), invasion of privacy, intrusion upon seclusion, conversion, and trespass to chattels.[33]

25. Geoff Duncan, *Open Letter Urges Facebook to Strengthen Privacy*, DIGIT. TRENDS (June 17, 2010), https://www.digitaltrends.com/computing/open-letter-urges-facebook-to-strengthen-privacy/.

26. Ian Paul, *Advocacy Group Asks Facebook for More Privacy Changes*, PC WORLD (June 17, 2010, 5:02 AM), https://www.pcworld.com/article/199099/facebook_privacy_fixes.html.

27. Nik Cubrilovic, *Logging Out of Facebook is Not Enough*, NIK CUBRILOVIC, https://nikcub.me/posts/logging-out-of-facebook-is-not-enough (modified Oct. 5, 2019).

28. *Id. See* Davis v. Facebook, Inc. (*In re* Facebook Internet Tracking Litig.), 956 F.3d 589, 596 (9th Cir. 2020).

29. Facebook, Inc., Commission Order Modifying Order, File No. 092-3184 (F.T.C. 2020). *See Davis*, 956 F.3d at 597 n.3.

30. *In re* Facebook Internet Tracking Litig., 844 F. Supp. 2d 1374 (J.P.M.L. 2012) (ordering the transfer and consolidation of eleven actions pending in various districts to the Northern District of California).

31. *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 927-28 (N.D. Cal. 2015).

32. *Id.* at 925.

33. *Id.* at 929; *Davis*, 956 F.3d at 597.

Facebook filed a motion to dismiss these claims for lack of standing and insufficient pleadings and the district court agreed, finding that although plaintiffs had standing to bring their claims arising under the SCA and Wiretap Act, they failed to adequately state a claim for relief under those statutes, and lacked standing to bring the rest of their claims. [34] After their first district court dismissal, plaintiffs were given leave to amend their first complaint, so they filed a second complaint with similar claims as well as added claims for breach of contract and breach of duty of good faith and fair dealing.[35] The claims in the second complaint were also dismissed, but plaintiffs were given leave to amend their claims for breach of contract and breach of duty of good faith.[36] Plaintiffs filed a third complaint which only contained their claims against Facebook for breach of contract and duty of good faith, but these claims were dismissed without leave to amend, exhausting the remedies available to the plaintiff class at district court.[37]

Plaintiffs appealed from their third and final dismissal at district court to the Ninth Circuit Federal Court of Appeals.[38] In *Davis v. Facebook, Inc.*, the Ninth Circuit held that the putative plaintiff class had standing to bring their claims against Facebook.[39] Although the Ninth Circuit found that the plaintiffs did not adequately plead their claims for violation of the SCA and breach of contract, they found the remaining claims adequately pleaded, including their claims against Facebook for violation the Wiretap Act and invasion of privacy.[40]

II. Legal Background and Court's Reasoning

The Ninth Circuit upheld in part and reversed in part the decision of the District Court for the Northern District of California by finding that the Plaintiffs had standing and were able to adequately plead claims for invasion of privacy, intrusion upon seclusion, trespass to chattels and fraud, statutory larceny, as well as claims brought pursuant to the Wiretap Act, CIPA, and Computer Data Access and Fraud Act; although the Plaintiffs did not have standing to bring their breach of contract and breach of implied covenant of good faith and fair dealing claims, or their claims brought pursuant to the SCA.[41]

34. *In re Facebook*, 140 F. Supp. 3d at 929-30.

35. *In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 840 (N.D. Cal. 2017).

36. *Id.* at 848.

37. *In re* Facebook Internet Tracking Litig., 290 F. Supp. 3d 916, 918, 922-23 (N.D. Cal. 2017).

38. *Davis*, 956 F.3d at 597.

39. *Id.* at 598.

40. *Id.* at 597-601, 608-11.

41. *Id.* at 597, 611.

A. The Ninth Circuit Held that the Plaintiffs Had Standing to Pursue their Claims for Invasion of Privacy, Intrusion Upon Seclusion, Breach of Contract, Breach of Good Faith, as well as Claims Under The Wiretap Act and the California Invasion Of Privacy Act (CIPA)

Article III of the U.S. Constitution limits the authority of the judicial branch to resolving "cases" and "controversies."[42] The doctrine of "standing" arises from this constitutional limitation and prevents federal court overreach by separating justiciable claims, which are within the purview of the judicial branch of government, from claims that the courts cannot resolve.[43] *Lujan v. Defenders of Wildlife* sets forth the test to determine whether plaintiffs have standing.[44] To establish standing, plaintiffs must fulfill three doctrinal elements: (i) their injury must be an injury in fact; (ii) the injury must be causally connected to the challenged conduct of the defendant; and (iii) it must be likely that their injury will be redressed by a favorable decision by the court.[45] For an injury to be an "injury in fact," it must be "concrete and particularized" as well as "actual or imminent."[46]

In *Davis v. Facebook, Inc.*, the Ninth Circuit affirmed the holding of the district court below that the plaintiffs had standing to pursue their claims for invasion of privacy, intrusion upon seclusion, breach of contract, breach of good faith, as well as their claims under the Wiretap Act[47] and the California Invasion of Privacy Act (CIPA).[48] CIPA is a California wiretapping law similar the Federal Wiretap Act, which protects internet users by creating a statutorily recognized right prohibiting others from intercepting one's electronic communications.[49] All of these claims related to the plaintiffs' privacy interest, which both the Ninth Circuit and the Northern District of California found were adequately alleged.[50] Plaintiffs alleged that Facebook tracked their potentially sensitive and personal internet browsing history and connected it with their personal Facebook profiles, creating a "cradle-to-grave" profile without users' knowledge or consent.[51] The Ninth Circuit found that Facebook's alleged data collection could deprive its users of the opportunity to

42. U.S. CONST. art. III, § 2, cl. 1.

43. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

44. 504 U.S. 555, 560-61 (1992).

45. *Id.*

46. *Id.*

47. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

48. 956 F.3d 589, 598 (2020); California Invasion of Privacy Act, CAL. PENAL CODE §§ 630-638.55.

49. *Davis,* 956 F.3d at 606-07 (describing the similarities between the federal wiretap act and CIPA); California Invasion of Privacy Act, CAL. PENAL CODE §§ 630-638.55; Kevin M. McGinty, *Alleged Wiretap Act and CIPA Violations Held to Satisfy Spokeo Test for Standing in Latest Gmail Privacy Class Action*, MINTZ (Oct. 3, 2016), https://www.mintz.com/insights-center/viewpoints/2016-10-03-alleged-wiretap-act-and-cipa-violations-held-satisfy-spokeo.

50. *Davis,* 956 F.3d at 598-99.

51. *Id.*

control or prevent Facebook's "exploitation of their private lives."[52] The plaintiffs alleged conduct by Facebook which clearly invaded their historically recognized right to privacy, so they had standing to pursue their privacy-related claims against Facebook.[53]

However, the district court and the Ninth Circuit disagreed on whether the plaintiffs had standing to bring their fraud-related state common law and statutory claims.[54] Plaintiffs' fraud-related claims required plaintiffs to demonstrate that some actual injury may have occurred, and plaintiffs could only recover the actual damages incurred from the Facebook's conduct.[55] Unlike other data privacy cases, plaintiffs alleged their browsing data had intrinsic value and was marketable, but they did not show that Facebook's use of the data prevented them from also selling it or diminished its value.[56] The district court reasoned that plaintiffs were not required to show economic harm to have standing for their their privacy-related claims, but the plaintiff class did not show the requisite economic harm or loss to bring their fraud-related claims against Facebook.[57]

The Ninth Circuit disagreed, finding that the plaintiffs had standing for their fraud-related state common law and statutory claims.[58] Under California law, plaintiffs have a legal interest in the profits unjustly earned by Facebook through use of their data, regardless of whether they planned to sell that data or whether its value was reduced by Facebook's use of it.[59] Plaintiffs alleged that their browsing history had economic value, and that Facebook used that information without their authorization.[60] Therefore, they sufficiently alleged that Facebook was unjustly enriched by using their data, which entitled them to the profits Facebook had unjustly earned and gave them standing for their fraud-related state claims.[61] With this holding, the Ninth Circuit supported an expansive view of standing for California state fraud-related claims in data privacy cases, allowing them to be brought even without showing economic injury.[62] Under the Ninth Circuit's reasoning, the unauthorized usage of this data does not just implicate privacy concerns, but also supports litigation against companies who unjustly enrich themselves by using the data without authorization.[63]

52. *Id.*
53. *Id.* at 599.
54. *Id.*
55. *Id.* at 599 n.4.
56. *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 931-32 (N.D. Cal. 2015).
57. *Id.*; *In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 842-43 (N.D. Cal. 2017).
58. *Davis*, 956 F.3d at 599-601.
59. *Id.*
60. *Id.*
61. *Id.* at 601.
62. *See id.*
63. *See id.*

B. The Ninth Circuit Held That the Plaintiffs Did Not Sufficiently Plead Claims for Intrusion Upon Seclusion, Invasion Of Privacy, and Violation of the Wiretap Act; Further, it was Held That the Plaintiffs Did Not Adequately Plead Claims Under the Stored Communications Act or Breach of Contract

In the district court's opinion below, all of the plaintiffs' claims that were not dismissed for lack of standing were dismissed for failure to adequately state a claim.[64] After holding that the plaintiffs had standing to bring all of their claims, the Ninth Circuit turned to whether the putative plaintiff class had sufficiently pleaded a claim for relief sufficient to bring their litigation against Facebook.[65] Standards for the adequacy of plaintiffs' claims for relief and Facebook's motion to dismiss those claims are set forth by the Federal Rules of Civil Procedure.[66] Subsequent case law clarifies the standard for a well-pleaded complaint.[67]

Under Rule 8(a)(2), plaintiffs, at the pleading stage, must show that they are entitled to relief from the court.[68] Supreme Court decisions have clarified that this claim for relief must be a "plausible claim for relief."[69] As shown by *Bell Atlantic Corporation v. Twombly*, mere conclusory allegations by the plaintiffs are not enough to withstand a Rule 12(b)(6) motion to dismiss.[70] Their claims must instead enable the court to infer more than the mere possibility of the defendant's misconduct, viewing all of the facts alleged by the plaintiffs in the light most favorable to them.[71]

The Ninth Circuit first evaluated to the plaintiffs' California state tort claims for intrusion upon seclusion and invasion of privacy.[72] These claims are considered together, and to establish these claims plaintiffs must plead that: (1) they have a reasonable expectation of privacy; and (2) the defendant's intrusion on that privacy was "highly offensive."[73]

64. *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 935-37 (2015).

65. *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 848-49; *In re* Facebook Internet Tracking Litig., 290 F. Supp. 3d. 916, 918 (N.D. Cal. 2017).

66. FED. R. CIV. P. 8(a)(2), 12(b)(6).

67. Ashcroft v. Iqbal, 556 U.S. 662, 678-79 (2009) (iterating a two-prong test that courts should use in evaluating whether a complaint is well-pleaded: (1) judges must separate the complaint's factual allegations from legal conclusions, and (2) judges must then assess whether the factual allegations "plausibly give rise to an entitlement to relief"); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 554-555 (2007) (holding that "[f]actual allegations must be enough to raise a right to relief above the speculative level"); Conley v. Gibson, 355 U.S. 41, 47 (1957) (noting that all the Federal Rules of Civil Procedure require is "'a short and plain statement of the claim' that will give the defendant fair notice of what the plaintiffs claim is and the ground upon which it rests").

68. FED. R. CIV. P. 8(a)(2), 12(b)(6).

69. *Ashcroft*, 556 U.S. at 678-79 (2009); *Twombly*, 550 U.S. at 554-555.

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

71. *Ashcroft*, 556 U.S. at 678.

72. Davis v. Facebook, Inc. (*In re* Internet Tracking Litig.), 956 F.3d 589, 601-06 (9th Cir. 2020).

73. *Id.* at 601 (citing Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 286-87 (2009)).

The Ninth Circuit found that plaintiffs sufficiently claimed they had a reasonable expectation of privacy.[74] The Court argued that plaintiffs plausibly claimed Facebook set a reasonable expectation, through language in its "Data Use Policy" and "Help Center" pages, that Facebook would not track its logged-out users, so plaintiffs had a reasonable expectation of privacy.[75] Also, Facebook collected all URL information from users visiting websites that used Facebook plugins, even data that was potentially sensitive, and Facebook did so without notifying users that browser cookies would track user internet activity after users had logged out of Facebook.[76]

Two past Ninth Circuit cases addressing similar issues held that users did not have an expectation of privacy when their Internet Protocol ("IP") and URL addresses were collected.[77] In *United States v. Forrester*, the Ninth Circuit reasoned that internet users do not have a reasonable expectation of privacy for their IP address information because they should know that their IP addresses are accessible by their internet service providers.[78] Also, likening IP addresses to phone numbers, the court in *Forrester* reasoned that IP addresses do not reveal the content of a message any more than phone numbers would.[79] However, the *Forrester* decision included in a footnote that users may have a reasonable expectation of privacy regarding URLs, which can contain sensitive information.[80]

Ninth Circuit opinion *Graf v. Zynga* seemingly disagreed with the footnote in *Forrester*.[81] In *Zynga*, the Ninth Circuit held that Facebook users playing video games made by Zynga while using Facebook did not have a reasonable expectation to privacy regarding their URL information when Zynga and Facebook were able to collect that information.[82] However, the Ninth Circuit reasoned that the URL information in *Zynga* was less sensitive than the URL information which *Forrester* foresaw as giving users a reasonable expectation of privacy.[83]

74. *Id.* at 602-06.

75. *Id.* at 601-02.

76. *Id.* at 603.

77. United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2008); *Graf v. Zynga Game Network, Inc. (In re Zynga Privacy Litig.)*, 750 F.3d 1098, 1107-09 (9th Cir. 2014).

78. *Forrester*, 512 F.3d at 510 (hearing a "challenge[to] the validity of computer surveillance that enabled the government to learn the to/from addresses[,] . . . IP addresses[,] . . . and the total volume of information transmitted to or from" the account of a defendant on trial for allegedly operating an ecstasy-laboratory).

79. *Id.*

80. *Id.* at n.6. This footnote reads "[s]urveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity." *Id.*

81. *Graf*, 750 F.3d at 1108-09.

82. *Id.* at 1109.

83. *Id.* at 1108-09.

As the Ninth Circuit points out in *Davis*, the URL information in *Zynga* was not problematic because it contained less potentially sensitive user data than that foreseen by the dicta in *Forrester*. [84] The URL information in *Davis* was more sensitive, and therefore distinguishable from that at issue in *Zynga*, allowing the plaintiffs to sufficiently plead an expectation of privacy that could survive a Rule 12(b)(6) motion to dismiss.[85] In *Davis*, the URL information collected included "full-string, detailed URLs," which Facebook could use to link internet activity to user profiles and even find out what search terms users had entered into a search engine like Google before reaching a web page.[86] The increased sensitivity of the data implicated in *Davis* distinguished it from the URL information in *Zynga*, giving plaintiffs in data a reasonable expectation of privacy.[87]

The Ninth Circuit then addressed whether the plaintiffs provided sufficient arguments that Facebook's data collection practices could be found to violate the Federal Wiretap Act and analogous California law CIPA.[88] Under the Wiretap Act, it is unlawful to intentionally intercept an electronic communication without authorization.[89] However, there is an exemption to the Wiretap Act—it does not impose liability on those who intercept communications they are "party" to, or those where their interception is consented to by one of the parties.[90] Facebook maintained that its collection of user data technically fell under the party exemption, so was not a violation of the Wiretap Act.[91]

If an internet user visits a web page, their browser sends a "GET request"—a message directing the website to display the information that the user enters in their browser's URL bar.[92] The GET request also sends the website a referer header with the user's URL information.[93] In *Davis*, when users visited web pages with Facebook plugins the Facebook plugins directed users' web browsers to duplicate and contemporaneously send GET request information to Facebook at the same time as their browsers sent GET requests to the website, the intended recipient.[94]

84. *Id.*; Davis v. Facebook, Inc. (*In re* Internet Tracking Litig.), 956 F.3d 589, 604-05 (9th Cir. 2020).

85. *Davis*, 956 F.3d at 605-06.

86. *Id.*

87. *Id.*

88. *Id.* at 606-08.

89. 18 U.S.C. § 2511(1).

90. *Id.* at § 2511(2)(d).

91. Brief for Appellee at 50-51, Davis v. Facebook, Inc. (*In re* Internet Tracking Litigation), 956 F.3d 589 (9th Cir. 2020) (No. 17-17486).

92. *HTTP Requests*, CODE ACAD., https://www.codecademy.com/articles/http-requests (last visited Nov. 5, 2020).

93. *Davis*, 956 F.3d at 607.

94. *Id.*

As noted in *Davis*, other federal courts of appeals have addressed this issue and were split on whether conduct like Facebook's could violate the Wiretap Act.[95] The First and Seventh Circuits have held that the Wiretap Act could be violated by the contemporaneous, unauthorized duplication and sending of internet communications, and that the recipient of the unauthorized duplicate communication could not invoke the "party" exemption from liability under the Wiretap Act.[96]

In the First Circuit case Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Privacy Litig.), Pharmatrak provided its "NETcompare" web service to pharmaceutical companies. [97] Pharmatrak had assured the pharmaceutical companies that the NETcompare system would not collect personal data about the patients.[98] However, without the pharmaceutical companies' or patients' knowledge, personal patient data was collected using the NETcompare system.[99] Pharmatrak collected user data by displaying images on the websites of pharmaceutical companies who used their NETcompare service.[100] Those images placed browser cookies on the computers of users visiting those websites and were able to track user internet activity, similar to Facebook's tracking of users through cookies with internet plugins in *Davis*.[101]

The First Circuit explained that courts analyzing claims under the Wiretap Act have differentiated between communications that are acquired while "in transit," which are interceptions under the Wiretap Act, from those acquired while "in storage," which are not.[102] This distinction has made some courts unsure exactly how to apply the Wiretap Act to internet communications, as they can both considered both "in transit" and "in storage" at the same time.[103] However, the First Circuit held that communications which are acquired "contemporaneous[ly]" with their sending, like the communications in *Blumofe* or Facebook's data collection in *Davis*, are "interception[s]" as defined by the Wiretap Act.[104]

The Seventh Circuit case *United States v. Szymuszkiewicz* also explains the liability for contemporaneous duplication of communications under the Wiretap

95. *Davis*, 956 F.3d at 607-08; *see* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Privacy Litig.), 329 F.3d 9, 22 (1st Cir. 2003); United States v. Szymuszkiewicz, 622 F.3d 701, 705-07 (7th Cir. 2010); *In re* Google Inc., 806 F.3d 125, 142-43 (3rd Cir. 2019).

96. *Blumofe*, 329 F.3d at 19-20; *Szymuszkiewicz*, 622 F.3d at 707.

97. *Blumofe*, 329 F.3d at 12 (discussing NETcompare, which "was marketed as a tool that would allow a company to compare traffic on and usage of different parts of its website with the same information from its competitors' websites").

98. *Id.*

99. *Id.*

100. *Id.* at 13-14.

101. *Id.* at 14.

102. *Id.* at 21.

103. *Id.* at 21-22.

104. *Id.* at 22.

Act.[105] In *Szymuszkiewicz*, a revenue officer set up his supervisor's e-mail client to duplicate and forward all received e-mails to the revenue officer's e-mail account.[106] The Seventh Circuit found that the e-mails were sent simultaneously from the server to the supervisor and the revenue officer.[107] Contemporaneous acquisition of those duplicate e-mails by the employee was an interception, exposing the employee to liability under the Wiretap Act.[108]

The Third Circuit, on the other hand, has disagreed, holding that conduct like Facebook's does not implicate the Wiretap Act.[109] The Third Circuit case *In re Google, Inc.* concerned third-party advertisements placed by Google on the internet.[110] Similar to Facebook's collection of user data in *Davis*, when the *In re Google* plaintiffs followed links in advertisements placed by Google, third-party browser cookies duplicated and collected the GET requests sent by their computers and compiled them into user internet histories.[111] Those cookies included third-party cookies placed by the advertisers, which were used to track and monitor individual users' web activity in order to deliver personalized advertisements.[112]

Google assured its users that they could block all of Google's browser cookies by enabling their "cookie blocker" on their Safari or Internet Explorer web browsers.[113] However, the browser cookie blockers had loopholes which allowed Google and advertisers to still place cookies on user computers, even with the blockers enabled.[114] When users visited websites through Google advertisements, code embedded by Google circumvented their cookie blocker programs and allowed third-party cookies to track users.[115]

The Third Circuit split from the First and Seventh Circuits, holding that Google's placement of browser cookies on user cookies that duplicated and sent user information to advertisers without user authorization did not violate the Wiretap Act.[116] Third-party advertisers were the "intended recipients" of the user information collected through their browser cookies, so the Third Circuit found they were party to the communication and therefore exempted from liability.[117] The Third Circuit stressed that the Wiretap Act is not necessarily intended to stop all

105. *Szymuszkiewicz*, 622 F.3d at 701.
106. *Id.* at 702-03.
107. *Id.* at 704.
108. *Id.* at 705-06.
109. *In re* Google Inc., 806 F.3d 125, 142-43 (3rd Cir. 2015).
110. *Id.* at 130.
111. *Id.*
112. *Id.* at 131.
113. *Id.* at 132.
114. *Id.*
115. *Id.*
116. *Id.* at 142-43.
117. *Id.*

fraud and does not provide an equitable remedy to plaintiffs.[118] Therefore, "parties" like the third-party advertisers in *In re Google* could be exempt from liability for their collection of duplicated and contemporaneously sent user data, even when they collected that data deceitfully.[119]

In *Davis*, the Ninth Circuit sided with the First and Seventh Circuits and disagreed with the Third Circuit by holding that the putative class of users had adequately pleaded their claim under the Wiretap Act.[120] The court in *Davis* found that the unauthorized duplication and contemporaneous sending of information like users' GET requests over the internet was an interception and that Facebook could not claim they were "party" to that contemporaneously sent information.[121] The Ninth Circuit reached this conclusion by examining the objectives of the Wiretap Act, as shown by its legislative history.[122] The "paramount objective of the [Wiretap Act] is to protect effectively the privacy of communications."[123] The Wiretap Act's legislative history also indicates that it aims to prevent "an unseen auditor" from accessing communications.[124] Exempting conduct like Facebook's would undermine the aims of the Wiretap Act by "allowing the exception to swallow the rule," permitting third parties to deceitfully intrude on communications.[125]

Unlike their Wiretap Act claims, the Ninth Circuit in *Davis* disagreed that plaintiffs had adequately pleaded a violation of the Stored Communications Act ("SCA").[126] Under the SCA, it is unlawful to gain unauthorized access to a "facility" where electronic communication services are provided and to obtain communications which are "electronically stored" in that facility without authorization.[127] Electronic storage includes "temporary, intermediate storage" of electronic communications "incidental to [their] transmission."[128] It also includes storage of electronic communications for "backup protection" purposes.[129]

Plaintiffs argued that the toolbar on their browsers, where they typed URL addresses of web pages they then searched for, is an electronic storage "facility" for purposes of the SCA, even though it often contains the URL information for less than a second.[130] They maintained that the URL information was stored in their

118. *Id.* at 143-44.

119. *Id.*

120. Davis v. Facebook, Inc. (*In re* Internet Tracking Litigation), 956 F.3d 589, 607-08 (9th Cir. 2020).

121. *Id.* at 608.

122. *Id.*

123. *Id.* (quoting Joffe v. Google, 746 F.3d 920, 931 (9th Cir. 2013)).

124. *Id. See* S. REP. NO. 90-1097, *as reprinted in* 1986 U.S.C.C.A.N. 2112, 2154, 2182.

125. *Davis*, 956 F.3d at 608.

126. *Id.* at 608-09.

127. 18 U.S.C. § 2701(a).

128. *Id.* § 2510(17).

129. *Davis*, 956 F.3d at 608.

130. *Id.* at 608-09.

browser toolbars "incidental to" its transmission, until the user sends the URL information to the website they intend to reach, so Facebook violated the SCA by accessing that information.[131] Plaintiffs also alleged that their browsing history information was stored for backup protection purposes, so was protected under the SCA[132]

Davis and other cases examining the Wiretap Act and SCA seem to suggest that it is difficult to bring claims under both the Wiretap Act and the SCA for unauthorized access of the same communications.[133] The First Circuit case Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Privacy Litig.) explains the storage-transit dichotomy—that some courts have found that communications in storage are not "interceptions," and that only communications in transit are protected by the Wiretap Act—while acknowledging that this framework has limited applicability to internet transmissions, which may be both in storage and transit simultaneously.[134] However, Seventh Circuit case *Szymuszkiewicz* emphasized Congress in passing the SCA did not repeal or replace any part of the Wiretap Act, and that both claims can be brought and enforced independently of each other.[135]

Even if it is possible to enforce both the Wiretap Act and SCA in some instances, the Ninth Circuit in *Davis* found that the plaintiffs had not adequately pleaded a claim under the SCA.[136] The Ninth Circuit found that communications at issue in *Davis*, the GET requests sent to Facebook, were not the same communications as those entered into the plaintiffs' toolbar.[137] Any URL information displayed on the plaintiffs' browser toolbars merely informed them of their browser's location on the internet, so was not "incidental" to the sending of the GET requests at issue, and therefore not protected by the SCA.[138]

The Ninth Circuit reasoned that, while the SCA was intended by Congress to be broadly construed, its legislative history indicates that it aims to protect against unauthorized access of communications stored in facilities owned by third parties.[139] The SCA usually only applies to cases involving a centralized data-management entity, like an external server, and unlike the browser toolbars alleged by Plaintiffs to be a "facility" under the SCA.[140] Plaintiffs' argument that their browsing histories preserved for backup protection were protected by the SCA was

131. *Id.* at 608.

132. *Id.*

133. *Id.* at 608-09; *see* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Privacy Litig.), 329 F.3d 9, 21-22 (1st Cir. 2003); United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010).

134. *Blumofe*, 329 F.3d at 21-22.

135. *Szymuszkiewicz*, 622 F.3d at 705.

136. *Davis*, 956 F.3d at 608-09.

137. *Id.* at 609.

138. *Id.*

139. *Id.*

140. *Id.*

similarly rejected by the Ninth Circuit. The court reasoned that browsing histories are not "communications," but instead merely records of URL addresses they had visited, so are not protected by the SCA.[141]

Finally, the Ninth Circuit reached the plaintiffs' breach of contract claims against Facebook.[142] Breach of contract has four elements: (1) existence of a contract between plaintiffs and Facebook; (2) plaintiffs' performance under that contract; (3) Facebook's breach of that contract; and (4) damages to plaintiffs caused by Facebook's breach of the contract.[143] The Ninth Circuit found that plaintiffs did not form a contract with Facebook that included any promise by Facebook to no track logged-out users, so their claim for breach of contract was not adequately pleaded.[144]

Plaintiffs alleged that they formed a contract with Facebook through Facebook's "Statement of Rights and Responsibilities" ("SRR").[145] The plaintiffs argued that their contract with Facebook also included Facebook's "Privacy Policy" (which Facebook renamed its "Data Use Policy" during the class period).[146] Facebook's SRR did not contain any promise not to track logged-out users, but when the litigation started it directed users to read the Facebook Privacy Policy.[147] Plaintiffs argued that this document was incorporated into the SRR and became part of their contract with Facebook.[148] The Court argued, however, that even if the Privacy Policy was incorporated into the SRR by language included in the SRR, there was no promise by Facebook in the version of the Privacy Policy that existed at the start of litigation to not track logged-out users.[149]

The later Data Use policy contained a promise by Facebook not to track logged-out users.[150] Plaintiffs argued that the Data Use policy established a separate contract between them and Facebook, but the Ninth Circuit disagreed.[151] A contract requires an exchange for a promise.[152] The promise plaintiffs aim to enforce in *Davis* is Facebook's promise in its Data Use Policy not to track its logged-out users.[153] However, the Ninth Circuit found that this promise by Facebook did not include an

141. *Id.*
142. *Id.* at 610.
143. *Id.*
144. *Id.* at 610-11.
145. *Id.* at 610.
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*

"exchange" by Facebook's users sufficient to form a contract.[154] There was no commitment by Facebook's users in return for that promise, so their claim for breach of contract was not adequately pleaded.[155]

Davis represents a win for Facebook users interested in preserving data privacy protections. The Ninth Circuit upheld in part, and reversed in part the decision of the District Court for the Northern District of California by finding that the Plaintiffs had standing and were able to adequately plead claims for invasion of privacy, intrusion upon seclusion, trespass to chattels and fraud, statutory larceny, as well as claims brought pursuant to the Wiretap Act, CIPA, and Computer Data Access and Fraud Act; although did not have standing to bring their breach of contract and breach of implied covenant of good faith and fair dealing claims, or their claims brought pursuant to the SCA.[156] Although the case has only made it past the pleading stage at this point, the opinion indicates an increase in the judiciary branch's efforts to step in as a protector for internet users.[157] The Judiciary will not be able to preserve data privacy protections alone though, and the *Davis* opinion also makes clear that the current statutory and regulatory frameworks in the United States are inadequate to properly protect personal information from Websites like Facebook.[158]

III. DISCUSSION

The decision in *Davis* has broad implications on privacy law and potentially heightens liability for websites that tracking user internet activity.[159] While *Davis* shows that courts are stepping forward to protect the online data privacy interests of internet users, courts opinions alone will not be enough to curb the tracking of these websites.[160] Governments, at the federal or state level, should consider broader legislative or regulatory schemes to protect the data privacy interests of internet users, looking to the European Union's General Data Protection Regulation (GDPR) and California's Consumer Protection Privacy Act (CCPA) as examples of such schemes.[161]

154. *Id.* at 610-11.

155. *Id.*

156. *Id.* at 611.

157. *See infra* Section III.B.

158. *See infra* Section III.C.

159. Erik Manukyan, *Summary: Ninth Circuit Permits Federal Wiretap Act Claim Against Facebook*, LAWFARE (Apr. 24, 2020, 8:00 AM), https://www.lawfareblog.com/summary-ninth-circuit-permits-federal-wiretap-act-claim-against-facebook. *See infra* Section III.A.

160. *See infra* Section III.B, III.C.

161. *See infra* Section III.C.

A. Implications of Davis on Websites Tracking the Activity of Their Users

Facebook, whose information-gathering practices are at issue in the *Davis* decision, is the largest social media site in the world.[162] In 2019, 69% (over two-thirds) of U.S. adults reported that they use Facebook, either online or through their mobile phone.[163] Facebook has international reach too: as of April 2020, Facebook has nearly 2.5 billion active users and is used by nearly two-thirds of the 3.81 billion active social media users worldwide.[164]

However, the reach of the decision in *Davis* extends far past Facebook alone. Other large social media companies whose data usage practices may be implicated by the Ninth Circuit's decision include Instagram, with 1 billion active monthly users; Snapchat, with 360 million monthly users; and Twitter, with 330 million monthly users.[165] Like Facebook, these other large social media companies are also headquartered in California.[166] California is within the Ninth Circuit's jurisdiction, so the Ninth Circuit's holding against Facebook in *Davis* will also affect future litigation against these other top social media companies.[167]

B. Efforts by Courts in Protecting Online Data Privacy of Internet Users

Davis shows that the Ninth Circuit (and district courts within the Ninth Circuit) will have more permissive pleading standards in consumer data privacy cases moving forward, which may increase the liability for social media sites that use browser cookies to track their users' data.[168] The Ninth Circuit's finding that unjust enrichment could confer standing to plaintiffs for their trespass to chattels claim and other California state fraud-based claims may also subject internet companies

162. Maryam Mohsin, *10 Social Media Statistics You Need to Know in 2021 [Infographic]*, OBERLO, https://www.oberlo.com/blog/social-media-marketing-statistics (last updated Apr. 5, 2021).

163. Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, is Mostly Unchanged Since 2018*, PEW RSCH. CTR. (Apr. 10, 2019), https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.

164. *Most Popular Social Media Platforms in 2020*, OBERLO, https://www.oberlo.com/statistics/most-popular-social-media-platforms (last visited Dec. 19, 2020).

165. Kristi Kellogg, *The 7 Biggest Social Media Sites in 2020*, SEARCH ENGINE J. (Feb. 3, 2020), https://www.searchenginejournal.com/social-media/biggest-social-media-sites/

(the monthly user amounts listed above reflect active monthly users as of February 2020).

166. *Id.*

167. *What is the Ninth Circuit?*, U.S. CTS. FOR THE NINTH CIR., https://www.ca9.uscourts.gov/judicial_council/what_is_the_ninth_circuit.php (last visited Dec. 19, 2020) [hereinafter *Ninth Circuit Jurisdiction*].

168. *See* Emily A. Jordan, *Sharing More Than You Thought: Facebook Cannot Assert the Party Exception to Avoid Liability Under the Wiretap Act*, 62 B.C. L. REV. E. SUPP. II-205, 223-25 (2021).

to greater liability.[169] The expansive view of standing adopted by the Ninth Circuit in *Davis* also signals that the Ninth Circuit is serious about protecting user data privacy from overreach by social media companies.[170] Such broad standing under California law, as interpreted by the Ninth Circuit, could have a negative effect on the many internet businesses based in the "silicon valley" technology hub of San Francisco, which are located in California and subject to federal appeals in the Ninth Circuit.[171]

C. The Role That Legislative and Regulatory Schemes Can Play in Protection of the Data Privacy Interests of Internet Users

The decision in *Davis* shows that current laws regulating the collection and use of user data are ambiguous, so a new legal framework is needed to ensure that consumers can keep their sensitive data private and are adequately informed of the tracking practices of websites they visit.[172] Broader legal protections could be implemented by amending and updating old and archaic statutes, like the Federal Wiretap Act statutes.[173] With their decision in *Davis*, the Ninth Circuit strengthens the Wiretap Act's applicability to user browser cookies, but also reflects the limitations of the decades-old statute's use in policing privacy violations that occur in newer technological contexts.[174] The original 1968 version of the Electronic Communications Protection Act (ECPA), which established the Wiretap Act, was enacted before the widespread use of computers to communicate, so it mainly

169. Benkat Balasubramani, *Ninth Circuit Reinstates Decade-Old Lawsuit Against Facebook For Tracking Logged-Out Users–In re Facebook Internet Tracking*, TECH. & MKTG. L. BLOG (Apr. 22, 2020), https://blog.ericgoldman.org/archives/2020/04/ninth-circuit-reinstates-decade-old-lawsuit-against-facebook-for-tracking-logged-out-users-in-re-facebook-internet-tracking.htm.

170. *Id.*

171. *Ninth Circuit Jurisdiction*, *supra* note 167.

172. Davis v. Facebook, Inc. (*In re* Internet Tracking Litigation), 956 F.3d 589, 604 (9th Cir. 2020) (noting examples of how courts have grappled with ambiguity in the current legal scheme, such as how to determine who qualifies as a "party" for purposes of the Wiretap Act's exemption from liability for those who are "party" to the communication).

173. *See* Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today – and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ (explaining how the pace of personal data found online has grown significantly over the past several years and laws cannot keep up, a significant overhaul of the current legal framework is needed).

174. *Davis*, 956 F.3d at 598 ("[T] he legislative history and statutory text demonstrate that Congress and the California legislature intended to protect these historical privacy rights when they passed the Wiretap Act, SCA, and CIPA [and] thus, these statutory provisions codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing."). *See also id.* at 608 (explaining how the SCA requires that Plaintiffs make a showing that the defendant internet company "gained unauthorized access to a 'facility'" where it accessed electronic communications in 'electronic storage[,]'" even though this means that many current data privacy claims will not be protected by the act).

dealt with oral communications by telephone—far different from the digital data at issue in *Davis*.[175]

In 1986 and through subsequent amendments, the ECPA was broadened to cover breaches of private data communications, either collected in real-time (protected by the Wiretap Act), or collected while in storage (protected by the Stored Communications Act ("SCA")). This distinction became more important in 1986, when the SCA was established, because computer storage was much more expensive.[176] However, computer storage has now become much cheaper and there is a less rigid distinction between "electronic storage" and real-time communication, which is instead protected by the Wiretap Act.[177] The similarity and overlap between stored communications and real-time communications provides an example of how courts struggle to conform the ECPA to new internet technologies.[178] A new amendment to the ECPA could help courts uniformly recognize the role user data plays in our society, so that they can better deal with current information technology realities that consumers may face.[179]

Another way to protect user privacy could be the enactment of new regulations to police websites' use of the data of their users. Recent regulatory schemes, like the European Union's General Data Protection Regulation (GDPR)[180] and California's Consumer Protection Privacy Act (CCPA),[181] have been enacted to protect web user privacy. While both regulatory schemes are focused on protecting consumer privacy by limiting the scope of when websites can sell users' data as well as increasing transparency requirements on those websites by imposing of penalties

175. Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 381 (2014).

176. *Id.* at 386, 391.

177. *Id.* at 391.

178. *Id.* at 395; *see* Michael E. Lackey & Oral Pottinger, *United States: Stored Communications Act: Practical Considerations*, MONDAQ (July 13, 2018), https://www.mondaq.com/unitedstates/privacy-protection/717180/stored-communications-act-practical-considerations ("[T]he SCA's age . . . makes it difficult to apply in modern times.").

179. *Electronic Communications Privacy Act*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/ecpa/ (last visited July 22, 2021) (mentioning that numerous amendments to the ECPA have been advocated for, "including an across-the-board warrant requirement, search notice and returns for users, protection of location data, and mandatory data minimization and end-to-end encryption for commercial e-mail services").

180. Ben Wolford, *What is the GDPR, the EU's New Data Protection Law?*, GDPR EU, https://gdpr.eu/what-is-gdpr/ (last visited Dec. 19, 2020) (describing the General Data Protection Regulation (GDPR) as "the toughest privacy and security law in the world" by imposing "harsh fines" on those found to be in violation of its standards, one example of which is only permitting businesses to collect data that is necessary for specified purposes and requiring business to impose appropriate data security measures).

181. California Consumer Privacy, Cal. Civ. Code §§ 1738 - 3273.16; *see also California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa (last visited Dec. 19, 2020) (explaining how the California Consumer Privacy Act (CCPA) protects data privacy by requiring that individuals be properly notified of what personal information businesses are collecting as well as requiring that businesses allow individuals to opt-out of having their personal information sold).

and fines on companies found to be in violation,[182] the CCPA and GDPR have some differences.[183] The CCPA protects a broader amount of user data than the GDPR—the GDPR only protects individual data, but the CCPA also extends to household data.[184] However, the GDPR gives more robust protections than the CCPA because the GDPR gives users the right to prior consent, requiring websites to disclose data use and gain consent from their users before using their users' data.[185] On the other hand, the CCPA merely gives users the right to opt-out of having their data used, only allowing users to protect their data after it has been used.[186]

The EU's GDPR provides a strong system of regulation ensuring user privacy,[187] but it does have some drawbacks.[188] The GDPR incidentally regulates web companies that may only have a few customers in the European Union, burdening even relatively small companies from other places in the world with the relatively higher cost of GDPR compliance.[189] While the strict requirements for compliance with the GDPR place new burdens on both large and small businesses, the GDPR's intense enforcement also ensures that web companies focus on cybersecurity and their handling of user data.[190] Increased focus by websites on cybersecurity risks and increased control given to consumers over how their data is used will also restore consumer trust in the web companies handling their personal data.[191] A strongly enforced and more extensive consumer privacy regulatory framework like the GDPR is also needed in the United States, and California's CCPA is a step towards that better system.[192]

More robust consumer privacy regulation and disclosure requirements would benefit both consumers and social media websites alike by increasing the transparency of social media companies using consumer data for profit and giving

182. *CCPA vs. GDPR – Differences and Similarities,* DATA PRIV. MANAGER (Aug. 01, 2020), https://dataprivacymanager.net/ccpa-vs-gdpr/.

183. *CCPA vs GDPR*, COOKIEBOT, https://www.cookiebot.com/en/ccpa-vs-gdpr/ (updated Nov. 30, 2020).

184. *Id.*

185. *Id.*

186. *Id.*

187. Wolford, *supra* note 180 (exploring some of the GDPR's requirements, such as requiring companies to implement measures to protect user data such as end-to-end encryption, or only allowing personal data to be processed in specific circumstances, such as when it is necessary to enter into a contract or may help save someone's life).

188. Eline Chivot, *Two Years On, the GDPR's Flaws Show Why the EU Should Avoid Additional Rules*, CTR. FOR DATA INNOVATION (June 24, 2020), https://datainnovation.org/2020/06/two-years-on-the-gdprs-flaws-show-why-the-eu-should-avoid-additional-rules/.

189. Lars Koudal, *GDPR Benefits – Pros and Cons*, CLEVER PLUGINS, https://cleverplugins.com/pros-cons-gdpr/ (last visited Dec. 19, 2020).

190. *Id.*

191. *Id.*

192. Bernard Gallagher, *Will the U.S. Adopt a Nationwide Data Privacy Law Similar to GDPR?*, I.S. PARTNERS, https://www.ispartnersllc.com/blog/us-nationwide-data-privacy-law-gdpr/ (updated Dec. 21, 2020).

consumers better control over what data they choose to share with internet companies.[193] Consumers have become more aware of cookies and their role in tracking user information. A 2006 report found that while over 90% of internet consumers claimed to know what internet cookies were, only 15.5% of those claiming they knew about cookies actually demonstrated even simple knowledge about internet cookies.[194] However, a 2012 survey found that much wider user knowledge about cookies, with 69% of respondents reporting that they were aware of internet cookies and how cookies are used to collect user data.[195]

Along with their heightened awareness of the role of browser cookies, consumers are now also more likely to limit or reject data collection by browser cookies. The 2012 study referenced above found that 73% of respondents regularly managed their browser's cookie settings.[196] Research from the fourth quarter of 2017 indicated that consumers either blocked or deleted 64% of the tracking cookies used by advertising firms for digital advertising.[197] This shows that consumers have low trust in internet cookies and are concerned about their privacy being encroached on by the websites they visit. More clear laws regulating social media companies' tracking of user data and more transparent required disclosure practices would address this concern.[198]

The ambiguity of the current legal framework policing user data privacy is also felt by social media companies themselves.[199] Web companies who fear liability under the Wiretap Act may have to defensively adopt new practices to ensure they properly disclose any tracking of their users.[200] In fact, third-party tracking cookies are being phased out of use by many websites, partly in response to new regulations

193. Karen Schuler, *Federal Data Privacy Regulation is on the Way – That's a Good Thing*, IAPP (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/.

194. Anthony D. Miyazaki, *Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage*, 27 J. OF PUB. POL'Y & MKTG. 19, 21 (May 2008), https://www.researchgate.net/publication/247837682_Online_Privacy_and_the_Disclosure_of_Cookie_Use_Effects_on_Consumer_Trust_and_Anticipated_Patronage.

195. Graham Charlton, *Just 23% of Web Users Would Say Yes to Cookies*, ECONSULTANCY (Apr. 16, 2012), https://econsultancy.com/just-23-of-web-users-would-say-yes-to-cookies/.

196. *Id.*

197. Ross Benes, *Web Browsers Reject About Two-Thirds of Cookies*, BUS. INSIDER INTEL.: EMARKETER (Mar. 27, 2018), https://www.emarketer.com/content/web-browsers-reject-about-two-thirds-of-cookies.

198. *See* Steve Sirich, *Data Transparency In the Age of Privacy Protection*, FORBES (Mar. 25, 2020, 7:30 AM), https://www.forbes.com/sites/forbescommunicationscouncil/2020/03/25/data-transparency-in-the-age-of-privacy-protection/?sh=6ba181be46b2.

199. Yaki Faitelson, *Why U.S. GDPR – Style Privacy Laws are Good for Business*, FORBES (Dec. 19, 2019, 8:15 AM), https://www.forbes.com/sites/forbestechcouncil/2019/12/19/why-u-s-gdpr-style-privacy-laws-are-good-for-business/?sh=37d7c1eb8756.

200. Manukyan, *supra* note 159.

like Europe's GDPR and California's CCPA.[201] For instance, Google Chrome, a popular internet browser, has unveiled a plan to end the use of third-party cookies entirely, which would hamper advertising agencies' efforts to track user data.[202]

However, Facebook's tracking of user internet history is considered first party, so may not completely cease with the death of third-party tracking cookies.[203] This highlights an of the asymmetry fostered by current consumer privacy regulations: they allow large companies like Facebook and Google, who already have first-party access to user information within the "walled gardens" of their online ecosystems, to continue accessing consumer data and using that data for profit, while smaller web companies may struggle to gain similar access.[204]

Better regulation of the use of user data for profit would encourage social media companies to be more honest about the relationship between their users' data and their advertising revenue.[205] As recently as 2018, Mark Zuckerberg, CEO of Facebook, has maintained that Facebook does not sell its users' data.[206] However, Facebook's internal documents revealed that it has allowed its business partners, like Amazon and Microsoft, to access its users' personal data in exchange for further integration of Facebook's social media services.[207] These partnerships and exchanges of data "underscore how personal data has become the most prized commodity of the digital age."[208] Yet Facebook and other internet companies must continue to downplay and obfuscate their use of user personal data for profit. In the wake of the privacy scandal discussed above, Facebook denied that it had not violated user privacy by giving its business partners access to the data, but also simultaneously acknowledged that they had to regain consumer trust in the wake of its many privacy scandals.[209] This reflects that the use of user data to generate

201. Dr. Augustine Fou, *No More Third Party Cookies, No Problemo*, FORBES (Aug. 31, 2020, 7:37 AM) https://www.forbes.com/sites/augustinefou/2020/08/31/no-more-third-party-cookies—-good-or-bad-news/?sh=604d72125948

202. *Id. See Building a More Private Web: A Path Towards Making Third Party Cookies Obsolete*, CHROMIUM BLOG (Jan. 14, 2020), https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html.

203. Owen Ray, *Tracking Cookies are Dead: What Marketers Can Do About It*, INVOCA (June. 22, 2020), https://www.invoca.com/blog/tracking-cookies-are-dead-what-marketers-can-do-about-it.

204. *Id.*

205. *See* Sirich, *supra* note 198.

206. Kalev Leetaru, *Facebook Still Doesn't Understand What Privacy Means*, FORBES (Dec. 5, 2018), https://www.forbes.com/sites/kalevleetaru/2018/12/05/facebook-still-doesnt-understand-what-privacy-means/?sh=120fae8a3cde.

207. Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, it Carved an Opening for Tech Giants*, THE N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

208. *Id.*

209. *Id.*

revenue exists in a legal gray area and needs to be clarified with a better regulatory system.[210]

A more transparent legal framework policing use of consumer data could give consumers better control over what data they share with the social media applications they use, leading to a more mutually beneficial and transparent relationship between social media companies' profitability and the data of their users.[211] The decision in *Davis* is a step in the right direction, toward a more transparent relationship between users and websites, because it acknowledges that user data is valuable and underscores the importance of giving users better control over what personal information of theirs share with the websites they use.[212] Consumers want to use social media applications like Facebook, while social media companies want to generate revenue with use data. If our laws acknowledge that user data has value and is controlled by the users, it will allow users to enter into transactions with websites implicating their data with full knowledge of the value of that data and a better ability to limit unauthorized data use.[213] Even if tracking cookies become outmoded, a better legal framework is needed to ensure that consumers can protect their privacy, one which does not ignore the inextricable link between social media companies' revenue and their use of personal user data.[214]

IV. Conclusion

By recognizing that the unauthorized use of user internet data can give plaintiffs standing for economic claims and can implicate the Federal Wiretap Act, the Ninth Circuit's decision in *Davis* could have broad ramifications on websites' liability for using cookies or internet plugins.[215] Although the case has only made it past the pleading stage at this point, the opinion indicates an increase in the Ninth Circuit's efforts to step in as a protector for internet users.[216] Courts alone will not be able to preserve data privacy protections though, and the *Davis* opinion makes clear that

210. *See* Faitelson, *supra* note 199.

211. *See* Sirich, *supra* note 198.

212. Davis v. Facebook, Inc. (*In re* Internet Tracking Litigation), 956 F.3d 589, 600-01 (9th Cir. 2020).

213. *See* Theodore "Theo" Forbath Morey & Allison Schoop, *Customer Data: Designing for Transparency and Trust,* HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (conducting a "conjoint analysis to determine what amount survey participants would be willing to pay to protect different types of information" and finding that in the United States, consumers would be willing to spend about $110.00 to protect their government ID, about $50.00 to protect their credit card information, and about $10.00 to protect demographic information).

214. *See* Kerry, *supra* note 173 (arguing in favor of "a more common law approach adaptable to changes in technology—to enable data-driven knowledge and innovation while laying out guardrails to protect privacy" and contending that any legislative changes could be modeled after the Consumer Privacy Bill of Rights, which emphasizes individual control, transparency, security, and accountability, among other factors).

215. *See supra* note Section III.

216. *See supra* note Section II.

the current statutory and regulatory frameworks in the United States are ambiguous inadequate to properly protect personal information from Websites like Facebook.[217] It may be time for state and federal governments to make drastic changes to our legal schemes regulating online data protection to create a system of laws that can better keep up with the times and changing technology.[218] Governments can look to the EU's General Data Protection Regulation (GDPR) and California's Consumer Protection Privacy Act (CCPA) for guidance and a place to start in devising such a system.[219]

217. *See supra* note Section III.

218. *See supra* note Section III.C.

219. *See supra* note Section III.C.