**BURSOR & FISHER, P.A.**
Philip L. Fraietta (State Bar No. 354768)
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: (914) 874-0708
Facsimile: (914) 206-3656
Email: pfraietta@bursor.com

*Counsel for Plaintiff*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

TAMMY KIRKPATRICK, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CROCS, INC.,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Plaintiff Tammy Kirkpatrick brings this action individually and on behalf of all others similarly situated against Defendant Crocs, Inc. ("Defendant" or "Crocs"). Plaintiff makes the following allegations pursuant to the investigation of her counsel based upon information and belief, except as to allegations specifically pertaining to herself, which are based on personal knowledge.

## NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all U.S. residents who accessed and navigated crocs.com (the "Website") and whose electronic communications were intercepted or recorded by advertising technology provided by Meta Platforms, Inc. ("Facebook" or "Meta") and Google, LLC ("Google") (together, the "Third Parties").

2. Crocs is a footwear retailer. Crocs uses its Website as an online marketplace where consumers can browse and purchase various products.

3. When consumers visit the Website, Defendant warrants to consumers that its Website cookies "do not store directly personal information[.]"

4. Unbeknownst to its customers, and contrary to its express assurance otherwise, Defendant intercepts and discloses its customers personally identifiable information ("PII"), and product purchase information to the Third Parties.

5. Defendant aids, agrees with, employs, or otherwise enables Third Parties to eavesdrop on communications sent and received by Plaintiff and Class Members on the Website that Defendant owns and operates, including communications that contain PII. By failing to procure consent, Defendant violated the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. §2511, *et seq.*); the California Invasion of Privacy Act ("CIPA") § 631–32, the California Comprehensive Computer Data Access and Fraud Act ("CDAFA") (Cal. Penal Code § 502, *et seq.*), and the California Constitution.

## PARTIES

***Plaintiff***

6. Plaintiff is a resident and citizen of Concord, California. At all relevant times, Plaintiff maintained active accounts with Facebook and Google. When creating her Facebook and

Google accounts, Plaintiff provided them with her PII, including her full name, date of birth, phone number, and email address. Plaintiff used the same device to access the Website that she did to access her Facebook and Google accounts. Plaintiff was in California when she visited the Website.

7. On or around November and December 2025, while within California, Plaintiff accessed Defendant's Website and purchased Crocs. Despite Defendant's representations of confidentiality, Plaintiff's communications during this visit were intercepted and disclosed to Third Parties through the Tracking Technologies, including communications that contained Plaintiff's identity (personal information) and purchase information. Neither Defendant nor the Third Parties procured Plaintiff's consent prior to these interceptions, nor was Plaintiff on notice of the fact that such interceptions were occurring. Such disclosures are a violation of Plaintiff's privacy and were done intentionally for targeted advertising purposes.

***Defendant***

8. Defendant Crocs, Inc. is a Delaware corporation with its headquarters in Broomfield, Colorado. Defendant owns and operates the Website.

9. Defendant knowingly and intentionally incorporated Tracking Technologies for marketing, advertising, and analytics purposes on the Website without disclosing the true extent of their functionality to its customers, including the tracking technologies provided by Third Parties.

10. Defendant configured the Tracking Technologies in a manner that discloses its customers'—including Plaintiff's—personally identifiable information despite expressly warranting that the Tracking Technologies would not do so.

## JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges that at least 100 people comprise the proposed class, that the combined claims of the proposed class members exceed $5,000,000 exclusive of interest and costs, and that at least one member of

the proposed class is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant conducts substantial business in California such that Defendant has significant, continuous, and pervasive contacts with California. Further, Plaintiff was residing in this District when she accessed the Website and had the Tracking Technologies intercept and disclose her personal information.

13. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b) because Defendant does substantial business in this District, a substantial part of the events giving rise to the claim occurred in this District, and Plaintiff resides in this District.

## FACTUAL ALLEGATIONS

### A. Defendant's Website and Privacy Representations

14. Defendant owns and operates the Website. Unbeknownst to customers, Defendant integrates tracking codes from Meta and Google into the Website (collectively the "Tracking Technologies").

15. "[W]ebsite owners often manipulate their privacy settings to make it harder for consumers to protect their privacy."[1]

16. "Cookies allow the websites to track user information for profiling and targeted advertising. The cookie consent notices will typically ask for consent to data collection and state how the data will be used. In this decision-making setting, users often have incomplete information regarding the cookie settings, which puts them at a disadvantage when compared with web designers."[2]

17. When users first accesses the Website, Defendant presents them with a prominent cookie banner wherein Defendant promises that it will keep their personally identifiable electronic communications confidential. Specifically, it warrants the Website's cookies "do not store direct personal information" and that they collect "aggregated" data that "does not directly identify you."

[1] Danyang Li, *The FTC and the CPRA's Regulation of Dark Patterns in Cookie Consent Notices*, 1 U. CHI. BUS. L. REV. 561 (2022) https://businesslawreview.uchicago.edu/print-archive/ftc-and-cpras-regulation-dark-patterns-cookie-consent-notices; Midas Nouwens et al., Dark Patterns After the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence, PROC. 2020 CHI CONF. ON HUM. FACTORS COMPUTING SYS. 1–13 (2020).

[2] *Id.*

> These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store direct personal information but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

**Figure 1**

> These cookies allow us to count and recognize traffic sources so we can measure the performance of our site. All information these cookies collect is aggregated and therefore does not directly identify you. If you do not allow these cookies, we will not know when you have visited our site and will not be able to monitor its performance.

**Figure 2**

18. Despite Defendant's claims it does not store directly personal information, Defendant enables the Third Parties to track consumers' Website browsing activities, including Plaintiff's, and eavesdrop on users' private communications on the Website.

19. As courts across the country have recognized, the identifiers that the Tracking Technologies capture—names, email address, phone number, and social media IDs—constitute "directly personal information." By capturing and storing this information, contrary to its explicit representation not to, Defendant fails to receive consent from customers to intercept their communications.

20. Through the advertising technology provided by the Third Parties, Defendant intercepts and discloses information about Plaintiff's and Class Members' identity and purchases. Defendant engages in this conduct despite clear promises not to do so.

### B. Consumers Have A Financial Stake In Companies' Promises Relating To Their Data Privacy

21. "In an era where every click, tap or keystroke leaves a digital trail, Americans remain uneasy and uncertain about their personal data and feel they have little control over how it's used."[3]

22. "The value of consumer data often comes from identifying users and combining their data from various sources. This is possible, in part, through the ubiquity of personally identifiable information (PII) and unique identifiers, as well as identifying individuals from non-PII, such as aggregated or anonymized data. The ability to identify users enables website and app operators to combine data and track user activity across devices."[4]

23. "Advertisers, as well as website and app operators, have incentives to improve their ad targeting by collecting detailed information about each user. Advertisers might expect more precise targeting to increase sales. Websites' revenue may depend on how frequently users click on the ad or how much time users spend viewing the ad."[5]

24. For retailers like Defendant, the ability to compile consumer patterns into algorithms improves how precisely they can sell to those same consumers.[6]

25. With increased surveillance of consumers' purchase patterns, consumer concern over the control of their data privacy has continued to grow:

- "86% of Americans are more concerned about their privacy and data security than the state of the U.S. economy – but two-thirds either don't know or are misinformed about how their data is being used and who has access to their

[3] Colleen McClain, Michelle Faverio, Monica Anderson, & Eugenie Park, *How Americans View Data Privacy*, PEW RESEARCH CENTER (October 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[4] CLARE Y. CHO & LING ZHU, CONG. RSCH. SERV., R47298, *Online Consumer Data Collection and Data Privacy*, (October 31, 2022), https://www.congress.gov/crs-product/R47298.

[5] Clare Y. Cho, CONG. RSCH. SERV., IF11448, *How Consumer Data Affects Competition Through Digital Advertising*, (January 26, 2023), https://www.congress.gov/crs-product/IF11448.

[6] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (example of how Target used consumer characteristics to identify and market to pregnant women).

privacy"[7]

- "67% of respondents don't understand what data privacy means or how their data is being used"[8]
- The public increasingly says they don't understand what companies are doing with their data. Some 67% say they understand little to nothing about what companies are doing with their personal data, up from 59%[9]
- 72% of Americans say there should be more [government] regulation than there is now; just 7% say there should be less. [10]
- Roughly four-in-ten Americans say they are *very* worried about companies selling their information to others without them knowing (42%) or people stealing their identity or personal information (38%).[11]
- 81% say they feel very or somewhat concerned with how companies use the data they collect about them. [12]
- People don't feel in control: Roughly three-quarters or more feel they have very little or no control over the data collected about them by companies (73%)[13]
- 36% strongly agree or somewhat agree they're in control of personal data. A third (29%) were concerned about how retailers and e-commerce companies use consumer data.[14]
- An overwhelming majority (85%) of consumers are taking at least one step to address their privacy and security concerns. However, 75% feel they should be doing more, and many indicate they feel a sense of powerlessness: They

---

[7] Gary Drenik, *Data Privacy Tops Concerns For Americans – Who Is Responsible For Better Data Protections?*, FORBES, (Dec. 8, 2023) https://www.forbes.com/sites/garydrenik/2023/12/08/data-privacy-tops-concerns-for-americans--who-is-responsible-for-better-data-protections/.

[8] *Id.*

[9] Colleen McClain, Michelle Faverio, Monica Anderson, & Eugenie Park, *How Americans View Data Privacy*, PEW RESEARCH CENTER, (Oct. 18, 2023) https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[10] *Id.*

[11] Colleen McClain, Michelle Faverio, Monica Anderson, & Eugenie Park, *Views of data privacy risks, personal data and digital privacy laws*, PEW RESEARCH CENTER, (Oct. 18, 2023) https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[12] *Id.*

[13] *Id.*

[14] *Survey Shows Consumers Concerned About Personal Data, Privacy and Internet Safety for Children,* KINETIC, (Jan. 24, 2025) https://www.windstream.com/blog/consumer-data-privacy-survey-2025.

believe that companies can track them no matter what they do (26%), don't know what actions they can take (25%), and think hackers can access their data no matter what they do (21%).[15]

26. This concern over data privacy also impacts consumer purchase behavior:

- 79% of Americans are concerned about how companies use their data.[16]
- 75% of Americans believe there should be more regulations to protect their privacy from companies collecting consumer data without their consent or knowledge.[17]
- 60% of users say they would spend more money with a brand they trust to handle their personal data responsibly.[18]
- 52% of American users chose not to use a product or service due to worries about how much personal data would be collected about them.[19]
- 48% of users have stopped buying from a company over privacy concerns.[20]
- 33% of users have terminated relationships with companies over data. They left social media companies, ISPs, retailers, credit card providers, and banks or financial institutions.[21]
- 81% of users say the potential risks they face from companies collecting data

[15] *New Deloitte Survey: Increasing Consumer Privacy and Security Concerns in the Generative AI Era*, DELOITTE, (Dec. 2, 2024) https://www.deloitte.com/us/en/about/press-room/increasing-consumer-privacy-and-security-concerns-in-the-generative-ai-era.html.

[16] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER, (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[17] Branka Vuleta, *18 Chilling Privacy Statistics in 2023*, LEGALJOBS (Jul. 22, 2025) https://legaljobs.io/blog/privacy-statistics.

[18] *Global Consumer State of Mind Report 2021,* TRUATA, https://www.truata.com/resources/report/global-consumer-state-of-mind-report-2021/.

[19] Andrew Perrin, *Half of Americans have decided not to use a product or service because of privacy concerns*, PEW RESEARCH CENTER, (Apr. 14, 2020) https://www.pewresearch.org/short-reads/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/.

[20] Ratnesh Pandey, *Staying Cyber-Secure While Working From Home*, TABLEAU, (updated Jul. 18, 2024) https://public.tableau.com/app/profile/ratnesh2928/viz/Stayingcyber-securewhileworkingfromhome/Stayingcyber-securewhileworkingfromhome/.

[21] *Consumer Privacy Survey*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf.

outweigh the benefits[22]

27. Consumer concerns over their privacy have been addressed at both the state and federal levels by the California Legislature and the Federal Trade Commission.

### C. The Federal Trade Commission and California Legislature's Protection of Consumer Data

28. The Federal Trade Commission has taken action "against dozens of companies that claimed to safeguard the privacy or security of users' information but didn't live up to their promises in the day-to-day operation of their business."[23]

29. Notably, the Federal Trade Commission seeks enforcement against companies who violate their representations about safeguarding consumer information:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.[24]

30. At the state level, the California Legislature is at the forefront of protecting citizens' privacy. Take, for example, the California Online Privacy Protection Act, requiring companies to "conspicuously post [their] privacy policy" and "[d]isclose whether other parties may collect personally identifiable about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service."[25] This statute also

---

[22] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER, (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[23] *Marketing Your Mobile App: Get It Right from the Start,* FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/marketing-your-mobile-app-get-it-right-start.

[24] *Privacy and Security* Enforcement, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[25] Cal. Bus. & Prof. Code § 22575(a).

defines "personally identifiable information ("PII")" as "[a] first and last name," "[a] home or other physical address," "[a]n e-mail address," "[a] telephone number," and "[a]ny other identifier that permits the physical or online contacting of a specific individual."[26]

**D. Overview of the California Invasion of Privacy Act and the Federal Wiretap Act**

31. The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

32. The California Supreme Court has repeatedly stated the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

33. Further, as the California Supreme Court has held in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

*Ribas*, 38 Cal. 3d at 360-61 (emphasis added; internal citations omitted); *see also Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021) (reaffirming *Ribas*).

34. As part of CIPA, the California Legislature introduced § 631(a), which imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978). Specifically, CIPA § 631(a) prohibits any person or entity from:

[26] Cal. Bus. & Prof. Code § 22575(a).

(i) "intentionally tap[ping], or mak[ing] any unauthorized connection . . . with any telegraph or telephone wire";

(ii) "willfully and without the consent of all parties to the communication . . . read[ing], or attempt[ing] to read, or to learn the contents or meaning of any . . . communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [California]"; or

(iii) "us[ing], or attempt[ing] to use . . . any information so obtained."

35. CIPA § 631(a) also penalizes those who "aid[], agree[] with, employ[], or conspire[] with" or "permit[]" "any person" to conduct the aforementioned wiretapping.

36. CIPA also outlaws "us[ing] an electronic amplifying or recording device to eavesdrop upon or record [a] confidential communication." Cal. Penal Code § 632. The term "confidential communications" means "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes . . . circumstances in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." Cal. Penal Code § 632(c).

37. Although CIPA was enacted before the dawn of the Internet, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.* 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013); *Javier v. Assurance IQ, LLC,* 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications").

38. This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.* 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

39. Individuals may bring an action against a violator of CIPA §§ 631 or 632 for $5,000 per violation. Cal. Penal Code § 637.2.

40. In a manner similar to CIPA, the Federal Wiretap Act (i.e. the ECPA) creates "a comprehensive scheme for the regulation of wiretapping and electronic surveillance."[27]

41. Although the ECPA does not apply "where one of the parties to the communication has given consent[,]" the ECPA eliminates the one-party consent exception when the conduct was for the "the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[28]

**E. The California Comprehensive Computer Data Access and Fraud Act**

42. The California State Legislature enacted the Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, *et seq.* in 2001 to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

43. The CDAFA makes it unlawful for "any person" to "[k]nowingly access[] and without permission take[], cop[y], or make[] use of any data from a computer, computer system, or computer network, or take[] or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2).

44. "Access," as defined by the CDAFA, means "to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1).

45. "Computer network," as defined by the CDAFA, means "any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities." Cal. Penal Code § 502(b)(2).

[27] *People v. Roberts*, 184 Cal. App. 4th 1149, 1167 (2010).

[28] 18 U.S.C. § 2511(d).

46. "Data," as defined by the CDAFA, means "a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Cal. Penal Code § 502(b)(6).

47. The CDAFA provides a private right of action: "[i]n addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Cal. Penal Code § 502(e)(1).

**F. Function of the Tracking Technologies**

48. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each device (such as a computer, tablet, laptop, or smartphone) accesses web content through a web browser (*e.g.*, Chrome, Safari, Edge, etc.).

49. Every website is hosted by a computer server that holds the website's contents and through which the entity in charge of the website exchanges communications with the consumer's device via web browsers.

50. Web communications consist of HTTP Requests and HTTP Responses and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- HTTP Request: an electronic communication sent from a device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

- Cookies: a small text file that can be used to store information on the device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.

- HTTP Response: an electronic communication that is sent as a reply to the device's web browser from the host server in response to a HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

51. A consumers' HTTP Request essentially asks the website to retrieve certain information (such as payment submissions and user selections), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the consumer's screen as they navigate the Website).

52. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

53. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. The Tracking Technologies embedded and configured on the Website by Defendant constitute source code.

**G. Meta's Tracking Technology**

54. Meta is one of the largest advertising companies in the country. To date, Meta generates nearly 98% of its revenue through advertising, [29] bringing in an excess of $160 billion in 2024.[30]

[29] Emmanuel Oyedegi, *Meta's ad business generated 98% of its total revenue in Q2 2025*, TECHLOY (Jul. 31, 2025) https://www.techloy.com/metas-ad-business-generated-98-percent-of-its-total-revenue-in-q2-2025/.

[30] Stacy Jo Dixon, *Meta's ad business generated 98% of its total revenue in Q2 2025*, STATISTA (Jan. 30, 2025) https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/?srsltid=AfmBOopC65RAw3WSm3y4ZtdYBpTiXhsmiFK7kSnFcm14WOV7esTu_uQ_.

55. Meta's advertising business began back in 2007 with the creation of "Facebook Ads," which was marketed as a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads." [31]

56. Today, Meta provides advertising on its own platforms, such as Facebook and Instagram, as well as websites outside these apps through the Facebook Audience Network. Facebook alone has more than 3 billion active users. [32]

57. Meta's advertising business has been extremely successful due, in large part, to Meta's ability to target people at a granular level. "Among many possible target audiences, [Meta] offers advertisers," for example, "1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'" [33]

58. Given the highly specific data used to target specific users, it is no surprise that millions of companies and individuals utilize Meta's advertising services. Meta generates substantially all of its revenue from selling advertisement placements:[34]

**Table 1:**

| Year | Total Revenue | Ad Revenue | % Ad Revenue |
|---|---|---|---|
| 2021 | $117.93 billion | $114.93 billion | 97.46% |
| 2020 | $85.97 billion | $84.17 billion | 97.90% |
| 2019 | $70.70 billion | $69.66 billion | 98.52% |
| 2018 | $55.84 billion | $55.01 billion | 98.51% |

59. One of Meta's most powerful advertising tools is the Meta Pixel, formerly known as the Facebook Pixel, which launched in 2015 and its SDK.

[31] Cecile Ho, *Announcing Facebook Pixel*, META (Oct. 14, 2015) https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/.

[32] Naveen Kumar, *Facebook Users Statistics (2025) – Latest Worldwide Data*, DEMANDSAGE (Aug. 19, 2015) https://www.demandsage.com/facebook-statistics/.

[33] Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, NEW YORK TIMES (Apr. 11, 2018) https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

[34] *Facebook Ad Revenue (2017–2027),* OBERLO, https://www.oberlo.com/statistics/facebook-ad-revenue.

60. Meta touted the Meta Pixel as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." According to Meta, to use Meta Pixel an advertiser need only "place a single pixel across [its] entire website to report and optimize for conversions" so that the advertiser could "measure the effectiveness of [its] advertising by understanding the action people take on [its] website."[35]

61. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users' activity as the users navigate through a website. As soon as a user takes any action on a webpage that includes the Meta Pixel, the code embedded in the page re-directs the content of the user's communication to Meta while the exchange of the communication between the user and website provider is still occurring.

62. Through this technology, Meta intercepts each page a user visits, what buttons they click, as well as specific information they input into the website and what they searched. The Meta Pixel sends each of these pieces of information to Meta with other identifiable information, such as the user's IP address. Meta stores this data on its own server, in some instances, for years on end.

63. This data is often associated with the individual user's Facebook account. For example, if the user is logged into their Facebook account when the user visits Defendant's Website, Meta receives third-party cookies allowing Meta to link the data collected by Meta Pixel to the specific Facebook user.

64. For example, Meta uses cookies named c_user, datr, fr and fbp to identify its account holders. Meta stores or updates Meta-specific cookies every time a person accesses their Facebook account from the same web browser.

65. The Meta Pixel can access these cookies and send certain identifying information like the user's Facebook ID to Facebook along with the other data relating to the user's website inputs.

[35] Cecile Ho, *Announcing Facebook Pixel*, META (Oct. 14, 2015) https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/.

66. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

67. A User's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the User's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

68. The Facebook datr cookie identifies the User's web browser. It is an identifier unique to each person's specific web browser and is another way Facebook can identify Facebook users.

69. The Facebook fr cookie is a combination of the Facebook ID (c_user) and the browser ID (datr) cookie values.

70. A User who accessed Defendant's Website while logged into (or recently having logged into) Facebook would have their browser transmit the c_user, datr and fr cookies to Facebook.

71. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.

72. Defendant intentionally configured the Tracking Technologies installed on its Website to capture both the "characteristics" of individual's communications with its Website (their IP addresses, Facebook ID, User-IDs, cookie identifiers, device identifiers, emails, and phone numbers) and the "content" of these communications (the buttons, links, pages, and tabs they click and view related to the shopping and products sought from Defendant).

73. Meta can also link the data to a specific user through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users, including Facebook users.

74. Lastly, Meta can link user data to individual users through identifying information collected through Meta Pixel using what Meta calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching, the website developer manually sends data to Meta to link users. Using Automatic Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.[36]

75. Importantly, even if Meta Pixel collects data about a non-Facebook user, Meta still retains and uses the data collected through Meta Pixel in its analytics and advertising services. These non-users are referred to as having "shadow profiles" with Meta.[37]

76. At the time Plaintiff used Defendant's Website, she maintained active social media account on Facebook. Plaintiff accessed the Website from the same device she used to visit Facebook, and Meta associated the data it collected about her from Defendant's Website with her Facebook account and other PII. Meta was also able to associate this information with her identity by matching hashed identifiers (name, phone, email, and address) to its own records.

77. Meta offers an analogous mobile version of the Meta Pixel known as an SDK to app developers. Meta's SDK allows app developers "to track events, such as a person installing your app or completing a purchase." By tracking these events developers can measure ad performance and build audiences for ad targeting.[38]

78. Meta's SDK collects three types of App Events. Automatically Logged Events are "log[] app installs, app sessions, and in-app purchases." Standard Events are "popular events that Facebook has created for the app." Custom Events are "events [the app developers] create that are specific to [the] app."[39]

[36] While Meta purports to "hash" the PII provided by users, Meta actually uses the hashed format *specifically to link the Meta Pixel data to Facebook profiles*.

[37] Jürgen Graf, *Investigating shadow profiles: The data of others*, TECHXPLORE (Sept. 22, 2023) https://techxplore.com/news/2023-09-shadow-profiles.html.

[38] *Meta App Event Tracking*, META, https://developers.facebook.com/docs/app-events/.

[39] *Meta App Event Tracking: Overview*, META, https://developers.facebook.com/docs/app-events/.https://developers.facebook.com/docs/app-events/overview.

79. Once the data intercepted through the Meta Pixel or SDK is processed, Meta makes this data available through its Events Manager and Ads Manager pages, along with tools and analytics to reach these individuals through future Facebook ads. For instance, this data can be used to create "custom audiences" to target the user, as well as other Facebook users who match members of the audiences' criteria.[40]

80. In addition to using the data intercepted through Meta Pixel and SDK to provide analytics services, Meta uses this data to improve its personalized content delivery, advertising network, and machine-learning algorithms, including by improving its ability to identify and target users.

81. Meta has no way to limit or prohibit the use of data collected through Meta Pixel and its SDK given Meta's open systems and advanced algorithms.

82. According to leaked internal Meta documents, one employee explained "You pour that ink [i.e., data] into a lake of water . . . at it flows . . . everywhere . . . How do you put that ink back in the bottle? How do you organize it again, such that it only flows to the allowed places in the lake?"[41]

83. In these same leaked documents, another employee explained Meta does "not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, that is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation."[42] Thus, once the data enters the Meta system, either through its SDK or Pixel, the data can be used for any and all purposes.

84. Meta's own employees confirmed no one at Meta can state confidently where all the data about a user is stored and used. In a recent court hearing as part of the Cambridge Analytica

[40] *Audience Network*, META, https://developers.facebook.com/docs/app-events/overview.https://developers.facebook.com/docs/audience-network/.

[41] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document*, VICE, (Apr. 26, 2022) https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes/.

[42] *Id.*

scandal of 2018, Meta's own engineers testified there was not a "single person" at Meta who could answer that question. [43]

85. Defendant uses at least the Meta Pixel on its Website. As a result, Defendant disclosed and Meta intercepted users' interactions on the Website, including Plaintiff's. Meta received at least the customer's name, email, location, and purchase information which it could associate with embedded cookies to further associate the information with the customer's profile. Meta and Defendant used this data, as well as other data uploaded directly to Meta by Defendant, so that Defendant could run advertisements using its services.

86. Plaintiff did not consent to the interception or disclosure of her data to Meta.

**H. Google's Tracking Technologies**

87. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over $1 trillion dollars. Google fancies itself a "tech" company, but Google, at its core, is an advertising company.

88. Google "make[s] money" from "advertising products [that] deliver relevant ads at just the right time," generating "revenues primarily by delivering both performance advertising and brand advertising." [44] In 2020, Google generated $146.9 billion in advertising revenue, which amounted to more than 80 percent of Google's total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

**Table 2:**

| Year | Total Revenue | Ad Revenue | % Ad Revenue |
|---|---|---|---|
| 2021 | $257.6 billion | $209.5 billion | 81.33% |
| 2020 | $182.5 billion | $146.9 billion | 80.49% |
| 2019 | $161.9 billion | $134.8 billion | 83.29% |
| 2018 | $136.8 billion | $116.5 billion | 85.12% |

[43] Isober Asher Hamilton, *Senior Facebook engineers say no one at the company knows where your data is kept*, BUSINESS INSIDER, (Sept. 8. 2022) https://www.businessinsider.com/meta-doesnt-know-where-all-your-data-is-engineers-say-2022-9#:~:text=Two%20Meta%20engineers%20were%20grilled,there%20for%20almost%20nine%20years.

[44] ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm.

89. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google's SDK and pixel integrate with Google's advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google's ad network and products increasing Google's overall ad revenue. Products like Google's SDK and its tracking pixel also improve the company's advertising network and capabilities by providing more wholesome profiles and data points on individuals.

90. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

91. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth information about user behavior. Also, Universal Analytics enabled tracking the same user across multiple devices through its addition of the User-ID feature, which "associate[s] a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices." [45]

92. In 2020, Google launched Google Analytics 4, a platform combining Google Analytics with Firebase to analyze both app and web activity.

93. Since launching Google Analytics, Google has become one of the most popular web analytics platforms on the internet. Indeed, Google had a $62.6 billion increase in advertising revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

[45] *About the User-ID feature*, GOOGLE, https://support.google.com/analytics/answer/3123662#zippy=%2Cin-this-article.

94. Google touts Google Analytics as a marketing platform that offers "a complete understanding of your customers across devices and platforms." [46] It allows companies and advertisers that utilize it to "understand how your customers interact across your sites and apps, throughout their entire lifestyle," "uncover new insights and anticipate future customer actions with Google's machine learning to get more value out of your data," "take action to optimize marketing performance with integrations across Google's advertising and publisher tools," and "quickly analyze your data and collaborate with an easy-to-use interface and shareable reports."[47]

95. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site—even when users are logged into their account portals. This code immediately intercepts a user's interaction with the webpage every time the user visits it, including what pages they visit and what they click on. The code also collects PII, such as IP addresses and device information related to the specific computing device a consumer (or users) is using to access a website. The device information intercepted by Google includes the user's operating system, operating system version, browser, language, and screen resolution.

96. In other words, when interacting with the Website, an HTTP Request is sent to Defendant's server, and that server sends an HTTP Response including the Markup that displays the website visible to the user and Source Code, including Google's tracking technologies.

97. Thus, Defendant is essentially handing its users a tapped device, and once the Webpage is loaded onto the users' browser, the software-based wiretap is quietly waiting for private communications on the Website to trigger the tap, which intercepts those communications intended only for the Defendant and transmits those communications to Google.

98. Once Google's software code collects the data intercepted from the Website, it packages the information and sends it to Google for processing. Google Analytics enables the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google database and cannot be changed.

[46] *Analytics*, GOOGLE, https://marketingplatform.google.com/about/analytics/.

[47] *Id.*

99. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on acquisition (*e.g.*, information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (*e.g.*, measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (*e.g.*, classify your users by age, location, language, and gender, along with interests they express through their online browsing and purchase activities).

100. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

101. The Website utilizes Google's pixel and SDK. As a result, Google intercepted users' interactions on the Website, including their PII. Google received at least "Custom Events" and URLs that disclosed the products purchased by the user. Google also received additional PII, including but not limited to the users' IP address, device information, and User-IDs by matching IP addresses, device information, and User-IDs it intercepts and linking such information to an individual's specific identity.

102. For example, the Website utilizes Google's "cid" or "Client ID" function to identify users as they navigate the Website.

103. Similarly, Google also utilizes the "auid" or "Advertiser User ID," and "guid" or "Globally Unique Identifier," cookies which identify unique users and unique interactions with a website Defendant sent these identifiers with each consumer's "event" data.

104. In addition to User-IDs, upon receiving information from the Website, Google also utilizes a "browser-fingerprint" to personally identify consumers. A browser-fingerprint is information collected about a computing device that is used to identify the specific device.

105. These browser-fingerprints are used to uniquely identify individual users when a computing device's IP address is hidden, or cookies are blocked, and can provide a wide variety of data.

106. As Google explained, "[w]ith fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites." [48]

107. The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques. Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.

108. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[49]

109. Browser-fingerprints are personal identifiers. Tracking technologies, like the ones developed by Google and utilized on the Website, can collect browser-fingerprints from website visitors.

110. As enabled by Defendant, Google collects vast quantities of consumer data through its tracking technology.

111. Due to the vast network of consumer information held by Google, Google matches the IP addresses, device information, User-IDs, and hashed versions of its account holders phone numbers and email addresses it intercepts and links such information to an individual's specific identity.

112. Google then utilizes such information for its own purposes, such as targeted advertising.

113. Google Analytics also links with Google Ads, allowing the data intercepted through Google Analytics to be utilized for targeted advertising purposes.[50] Such practices were in effect on the Website for targeted advertising purposes.

---

[48] Justin Schuh, *Building A More Private Web*, GOOGLE, https://blog.google/products-and-platforms/products/chrome/building-a-more-private-web/.

[49] *New reliable technique to track web users across browsers*, SCIENCEDAILY, https://www.sciencedaily.com/releases/2017/02/170213131447.htm.

[50] https://support.google.com/analytics/answer/9379420?hl=en#zippy=%2Cin-this-article.

114. The DoubleClick API "is an integrated ad technology platform that enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns."

115. DoubleClick was acquired by Google in 2008. In 2018, the DoubleClick API was integrated with the Google Analytics API into the Google Marketing Platform.[51] The Google Marketing Platform makes use of most of DoubleClick's features, albeit under different brand names: for example, "DoubleClick Bid Manager is now Display & Video 360," "DoubleClick Search is now named Search Ads 360," and DoubleClick Campaign Manager and DoubleClick Studio are now named Campaign Manager and Studio, respectively."[52]

116. As relevant here, however, data is still sent from the Website to Google through the DoubleClick API, and app developers like Defendant can then use the Google Marketing Platform to manage the data.

117. Once integrated into a developer's mobile application, the DoubleClick API allows an app developer to, among other features, analyze and optimize marketing campaigns and conduct targeted advertising. [53]

118. Once Defendant intercepts the Website communications through the DoubleClick API and discloses such information to Google (in real time), Google has the capability to use such information for its own purposes. "Google uses the information shared by sites and apps to deliver [] services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on [] partners' sites and apps." [54]

119. For example, Google utilizes the "auid" or "Advertiser User ID" cookies which identify unique users and unique interactions with a website.

120. Google also encodes the user's email address, to later match it to its own records.

---

[51] Brad Bender, *Introducing Google Marketing Platform*, GOOGLE MARKETING PLATFORM (June 27, 2018), https://www.blog.google/products/marketingplatform/360/introducing-google-marketing-platform/.

[52] *Introducing Google Marketing Platform*, GOOGLE, https://support.google.com/displayvideo/answer/9015629?hl=en.

[53] *DoubleClick Digital Marketing*, GOOGLE, https://support.google.com/faqs/answer/2727482.

[54] *Privacy and Terms*, GOOGLE, https://policies.google.com/technologies/partner-sites.

121. Google's range of SaaS services is based on Google's ability to collect and analyze information about consumers' web behavior and deliver targeted advertising to select consumers based on their web habits. This involves collecting visitor information from thousands of websites and then analyzing that information to deliver targeted advertising and group web users so that they can be targeted for products and categories they are interested in.

122. Information from websites, including Defendant's, is central to Google's ability to successfully market their advertising capabilities to future clients.

123. In sum, Google uses website communications to: (i) improve its own products and services; (ii) develop new Google for Business and Google Analytics products and services; and (iii) analyze website visitors' communications to assist with data analytics and targeted advertising.

124. Google views and processes every piece of information collected from the DoubleClick API, including the information collected from Defendant's Website, and uses it to assist with data analytics, marketing, and targeted advertising.

125. Google partners with Defendant in its marketing efforts. Google's tracking technologies, including Google Analytics, browser fingerprinting, and Google DoubleClick are employed on the Website in the manner described throughout this Complaint.

126. Plaintiff did not consent to the interception or disclosure of her data to Google.

**I. Defendant's Use of Tracking Technologies**

127. Pursuant to agreements with Meta and Google, Defendant intentionally and voluntarily embedded the Tracking Technologies on the Website. As illustrated within this section, Defendant unlawfully disclosed its customers'—including Plaintiff's—personally identifiable information to Third Parties through Tracking Technologies, without customer consent.

128. The Tracking Technologies are Source Code that do just that—they surreptitiously transmit a Website User's communications and inputs to the corresponding user IDs, much like a traditional wiretap.

129. For example, when individuals visit Defendant's Website via an HTTP request to Defendant's server, Defendant's server sends an HTTP response (including the Markup) that

displays the webpage visible to the User, along with Source Code (including the Tracking Technologies).

130. Once a webpage is loaded into the user's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Tracking Technologies, which then intercept those communications—intended only for Defendant—and instantaneously transmit those communications to the Third Parties.

131. For example, when individuals visit Defendant's Website via an HTTP request to Defendant's server, Defendant's server sends an HTTP response (including the Markup) that displays the webpage visible to the User, along with Source Code (including the Tracking Technologies).

132. The Third parties offer companies, including Defendant, snippets of code they can install in web browsers of users accessing their services. These code snippets uniquely identify the user and are sent with each intercepted communication to ensure the third party can identify the specific user associated with the information intercepted (in this case, confidential PII and purchase information).

133. Defendant intentionally configured the Tracking Technologies installed on its Website to capture both the "characteristics" of individual's communications with its Website (their IP addresses, Facebook ID, User-IDs, cookie identifiers, device identifiers, names, emails, phone numbers, and purchase information) and the "content" of these communications (the buttons, links, pages, and tabs they click, and view related to the shopping and products sought from Defendant).

134. Defendant installs these Tracking Technologies despite its understanding that its customers reasonably anticipate their identifiable information to be kept confidential and undisclosed to Third Parties. This installation contradicts Defendant's promise to keep PII non-personally identifiable.

135. Contrary to its promises, as soon as consumers enter Defendant's Website, Defendant begins tracking and disclosing their interactions with the Website to the Third Parties, including their personally identifiable information.

136. When users access the Website, Defendant discloses the URLs and page titles of every page that they visit, including during the checkout process. The URLs and page titles disclose what type of product the user is seeking to purchase. For example, when a consumer clicks on a product, the URL of the page for that product, which includes information about the product is shared, is shared with Third Parties as enabled by Defendant. The Third Parties also receive information when the consumer adds the product to their cart before checkout, and when they add their payment info. *See, e.g. See e.g.* Figs. 3-5 (Meta Interception); Figs. 6-7 (Google Interception).

137. An example illustrates the point. When a customer views a product and adds it to their cart and subsequently checks out for their purchase, Meta receives detailed information about the product, the price, and the purchaser. *See e.g.* Figs. 3-5.

| | |
|---|---|
| id | 283061001901751 |
| ev | SubscribedButtonClick |
| dl | https://www.crocs.com/p/specialist-ii-work-clog/204590.html?cgid=men-footwear-clogs&cid=001 |
| rl | https://www.crocs.com/c/men/footwear/clogs?origin=category&start=0&sz=36 |
| if | false |
| ts | 1782999543295 |
| iw | false |
| cd[buttonFeatures] | {"classList":"ok-button ","destination":"","id":"","imageUrl":"","innerText":"Add to Cart","numChildButtons":0,"tag":"button","type":"button","name":"","value":""} |
| cd[buttonText] | Add to Cart |
| cd[formFeatures] | [] |
| cd[pageFeatures] | {"title":"Specialist II Work Clog - Crocs "} |

| | |
|---|---|
| id | 283061001901751 |
| ev | SubscribedButtonClick |
| dl | https://www.crocs.com/on/demandware.store/Sites-crocs_us-Site/default/COCheckout-Step |
| rl | https://www.crocs.com/on/demandware.store/Sites-crocs_us-Site/default/Cart-Show |

neUS Minor IslandsUruguayBr","Tina Wiles50 SW 10th St Apt 1001Miami, FL 33130-4139US(954) 667-8899","Billing Last Name *","Use Shipping Address for BillingTina Wiles50 SW 10th St Apt 1001Miami, FL 33130-4139USyyy222@yahoo.com(954) 667-8899Billing AddressBilling Country *United StatesArgentinaAmerican SamoaAustraliaBrazilBelarusCanadaSwitzerlandChinaColombiaCost

**Figures 3-5**

138. In addition to intercepting consumers' communications throughout the checkout process, Meta's tracking technology on the Website also intercepts various cookie identifiers, including the sb, datr, c_user, xs, and fr cookies. The c_user cookie, which it associates with

various communications and events, is the equivalent of a user identification number unique to each Facebook user.

139. The same holds true with Google's Tracking Technologies. As Plaintiff and other users navigate the checkout process, Defendant intercepts and discloses product details and personally identifiable information (i.e. user email address and auid parameter) to Google through Google's Tracking Technologies. Google associates all this information with its unique identifier, the auid, and various tracking cookies. The purchaser's email is intercepted in an encoded format, which Google can decode.

| | |
|---|---|
| guid | ON |
| async | 1 |
| en | review_order |
| gtm | 45be66u1v890386512za200zb880616116zd880616116xec |
| gcd | 13l3l3l3l1l1 |
| dma | 0 |
| tag_exp | 115938466~115938469~119027224~119576881~119576885~119576891~119576895 |
| u_w | 2560 |
| u_h | 1441 |
| url | https://www.crocs.com/on/demandware.store/Sites-crocs_us-Site/default/COCheckout-Step |
| ref | https://www.crocs.com/on/demandware.store/Sites-crocs_us-Site/default/Cart-Show |
| rcb | 0 |
| frm | 0 |
| tiba | Checkout |
| did | dYmQxMT |
| gdid | dYmQxMT |
| currency_code | USD |
| hn | www.googleadservices.com |

**Figure 6**

| | |
|---|---|
| tag_exp | 115938466~115938469~119027224~119576881~119576885~119576891~119576895 |
| gclaw_src | 0_1 |
| rcb | 0 |
| did | dYmQxMT |
| gdid | dYmQxMT |
| npa | 0 |
| frm | 0 |
| gclgs | 1 |
| gclst | 2064399407 |
| gcllp | 57781624 |
| gclaw | Cj0KCQjw0JnRBhDJARIsALobnXZ7Zb6BqaGlqr-uhR2Sg49psOffCzCKh2N7vhQfmeQUOAirnNzWkJIaAkTbEALw_wcB |
| pscdl | noapi |
| auid | 1053337277.1780871417 |
| uaa | x86 |
| uab | 64 |
| uafvl | Google%20Chrome;149.0.7827.201\|Chromium;149.0.7827.201\|Not)A%3BBrand;24.0.0.0 |
| uamb | 0 |
| uam | |
| uap | Windows |
| uapv | 19.0.0 |
| uaw | 0 |
| ec_mode | c |
| _tu | IA |
| em | tv.1~em.2c837ce4e8c21d834c1bf37a9a24a1a27bf2355f4ce54fa9a21ea07ba835a0ba |
| ecsid | 507131274.1782998359 |
| emd | tvd.1~i1.fem.mc.p1 |

**Figure 7**

### J. Defendant Did Not Anonymize Consumer Data By Disclosing "Hashed" Values To Third Parties

140. The Federal Trade Commission routinely evaluates privacy representations by companies. When it comes to hashing the FTC has said the following:

> Companies often claim and act as if data that lacks clearly identifying information is anonymous, but data is only anonymous when it can never be associated back to a person. If data can be used to uniquely identify or target a user, it can still cause that person harm.
>
> One way that companies obscure personal data is through "hashing." Hashing involves taking a piece of data—like an email address, a phone number, or a user ID—and using math to turn it into a number (called a hash) in a consistent way: the same input data will always create the same hash.
>
> . . .

> This logic is as old as it is flawed – hashes aren't "anonymous" and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized. FTC staff will remain vigilant to ensure companies are following the law and take action when the privacy claims they make are deceptive.[55]

141. Thus, through the tracking technologies provided by the Third Parties, Defendant intercepted and disclosed Plaintiff and Class Members personally identifiable information regardless of whether it was hashed or in plain text.

## CLASS ALLEGATIONS

142. **Class Definition:** Plaintiff brings this action individually and on behalf all others similarly situated, as set forth below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure:

> The **Nationwide Class** that Plaintiff seeks to represent is defined as:
> All individuals residing in the United States who made a purchase on the Website during the Class Period.
>
> The **California Subclass** that Plaintiff seeks to represent is defined as:
> All individuals residing in California who made a purchase on the Website during the Class Period.

143. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgment.

144. The Nationwide Class and California Subclass are referred to collectively as the "Classes."

145. Excluded from the proposed Classes are Defendant; any affiliate, parent, or subsidiary of Defendant, any entity in which Defendant has a controlling interest; any officer, director, or employee of Defendant, any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

---

[55] *No, hashing still doesn't make your data anonymous*, FEDERAL TRADE COMMISSION (Jul. 24, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

146. Plaintiff reserves the right to amend the definitions of the Class or Subclass and add subclasses if further information and discovery indicate that the definitions should be narrowed, expanded, or otherwise modified.

147. **Numerosity:** Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff at this time. However, it is estimated that there are hundreds of thousands of individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's records and third-parties Meta and Google's records.

148. **Existence and Predominance of Common Questions of Fact and Law:** There is a well-defined community of interest in the questions of law and fact involved affecting the members of the proposed Classes. The questions of law and fact common to the proposed Classes predominate over questions affecting only individual class members. Such questions include, but are not limited to, the following:

(a) Whether Defendant's acts and practices violated the ECPA.

(b) Whether Defendant's acts and practices violated CIPA § 631;

(c) Whether Defendant's acts and practices violated CIPA § 632;

(d) Whether Defendant's acts and practices violated the CDAFA;

(e) Whether Defendant's acts and practices violated the privacy rights of Plaintiff and members of the California Class under the California Constitution; and

(f) Whether Plaintiff and members of the proposed Classes are entitled to damages, reasonable attorneys' fees, pre-judgment interest and costs of this suit.

149. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Classes because the Plaintiff, like all other class members, visited the Website and had her confidential electronic communications intercepted and disclosed to Third Parties.

150. **Adequacy:** Plaintiff is an adequate representative of the Classes because her interests do not conflict with the interests of the Classes she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this

action vigorously. The interests of the Classes will be fairly and adequately protected by Plaintiff and her counsel.

151. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of the Classes. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues. Finally, Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making it appropriate for this Court to grant final injunctive relief and declaratory relief with respect to the Classes as a whole.

## CAUSES OF ACTION

### COUNT I
**Violation Of The Electronic Communication Privacy Act,**
**18 U.S.C. § 2511, *et seq.***
**(On Behalf of the Nationwide Class)**

152. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

153. Plaintiff brings this claim on behalf of herself and members of the Nationwide Class.

154. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

155. The ECPA protects both the sending and the receipt of communications.

156. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

157. The transmission of Plaintiff's sensitive and personal information to Defendant's website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

158. The transmission of PII between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

159. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

160. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

161. The ECPA defines "electronic, mechanical, or other device," as "any device . . . which can be used to intercept a[n] . . . electronic communication[.]" 18 U.S.C. § 2510(5).

162. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Defendant and Meta used to track Plaintiff's and Class Members' communications while they were navigating the Website;

b. The computer codes and programs Defendant and Google used to track Plaintiff's and Class Members' communications while they were navigating the Website;

c. Plaintiff's and Class Members' browsers;

d. Plaintiff's and Class Members' mobile devices;

e. Defendant's and Google's web and ad servers;

f. Defendant's and Meta's web and ad servers;

g. The plan that Defendant and Meta carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website; and

h. The plan that Defendant and Google carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website.

163. Plaintiff's and Class Members' interactions with Defendant's website are electronic communications under the ECPA.

164. By utilizing and embedding the tracking technologies provided by the Third Parties on the Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

165. Specifically, Defendant intercepted—in real time—Plaintiff's and Class Members' electronic communications via the tracking technologies provided by the Third Parties on its website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and sensitive and personal information to the Third Parties.

166. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding their PII, including their identities and information related to their purchase on the Website. This confidential information is then monetized for targeted advertising purposes, among other things.

167. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to the Third Parties through the Tracking Technologies, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

168. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class members' electronic communications, while knowing or having reason to know that the

information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

169. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy and associating the content of Plaintiff's and Class members' electronic communications with preexisting consumer profiles and using the contents of their electronic communications in a manner that exceeds what Defendant promised Plaintiff and Class members on its Website.

170. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

171. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may award statutory damages to Plaintiff and Class Members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future; reasonable attorney's fees; and other litigation costs reasonably earned.

## COUNT II
**Violation Of The California Invasion Of Privacy Act,**
**Cal. Penal Code § 631**
**(On Behalf of the California Subclass)**

172. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

173. Plaintiff brings this claim against Defendant individually and on behalf of the California Subclass.

174. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630–638. CIPA begins with its statement of purpose—namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in

science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . .” Cal. Penal Code § 630.

175. A person violates California Penal Code § 631(a), if:

> By means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

176. Further, a person violates § 631(a) if s/he “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned” in the preceding paragraph. *Id.*

177. To avoid liability under § 631(a), a defendant must show it had the consent of <u>all</u> parties to a communication.

178. At all relevant times, Defendant aided, agreed with, and conspired with the Third Parties to track and intercept Plaintiff’s and Class Members’ internet communications while accessing the Website. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

179. Defendant, when aiding and assisting the Third Parties’ wiretapping and eavesdropping, intended to help the Third Parties learn some meaning of the content in the URLs and the content the visitor requested.

180. The following items constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA, and even if they do not, the Tracking Technologies fall under the broad catch-all category of “any other manner”:

(a) The computer codes and programs the Third Parties used to track Plaintiff and Class Members' communications while they were navigating the Website;

(b) Plaintiff's and Class Members' browsers;

(c) Plaintiff's and Class Members' computing and mobile devices;

(d) Defendant's and Google's web and ad servers;

(e) Defendant's and Meta's web and ad servers;

(f) The web and ad-servers from which the Third Parties tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate the Website;

(g) The computer codes and programs used by the Third Parties to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit the Website; and

(h) The plan the Third Parties carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to visit the Website.

181. The information that Defendant transmitted using Tracking Technologies constituted sensitive and confidential personally identifiable information.

182. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting the Third Parties to receive its customers' sensitive and confidential online communications through the Website without their consent.

183. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, $5,000 per violation or three times the amount of actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered or be threatened with, actual damages." Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

**COUNT III**
**Violation Of The California Invasion Of Privacy Act,**
**Cal. Penal Code § 632**
**(On Behalf of the California Subclass)**

184. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

185. Plaintiff brings this claim against Defendant individually and on behalf of the California Subclass.

186. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication.

187. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

188. The data collected on Defendant's Website constitutes "confidential communications," as that term is used in Section 632, because class members had an objectively reasonable expectation of private with respect to their personally identifiable information.

189. Plaintiff and Class Members expected their communications to Defendant to be confined to Defendant in part, because of Defendant's consistent representations that these communications would remain confidential. Plaintiffs and Class Members did not expect the Third Parties to secretly eavesdrop upon or record this information and their communications.

190. The Tracking Technologies from Third Parties, are all electronic amplifying or recording devices for purposes of § 632.

191. By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential communications to Defendant through this technology, the Third Parties eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

192. At no time did Plaintiff or Class members consent to Defendant or Third Parties conduct, nor could they reasonably expect that their communications to Defendant would be overheard or recorded by Third Parties.

193. The Third Parties utilized Plaintiff's and Class members' personally identifiable information for their own purposes, including advertising and analytics.

194. Defendant is liable for aiding and abetting violations of Section 632 by the Third Parties.

195. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Members of the California Subclass have been injured by the violations of Cal. Penal Code § 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

**COUNT IV**
**Violation of the Comprehensive Data Access and Fraud Act ("CDAFA")**
**Cal. Penal Code § 502, *et seq.***
**(On Behalf of the California Subclass)**

196. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

197. Plaintiff brings this claim individually and on behalf of the Class.

198. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or criminal action, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

199. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiff's and Class members' data.

200. Plaintiff and Class members suffered economic injury because Defendant unjustly profited from Plaintiff's personal information.

201. It would not be equitable to allow Defendant to keep those profits, which were generated by violating Plaintiff's privacy interests.

202. As a direct and proximate result of Defendant's unlawful conduct within the meaning of Cal. Penal Code § 502, Defendant has caused loss to Plaintiff and the Class members in an amount to be proven at trial.

203. Plaintiff, on behalf of herself, and the Class members, seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declaratory, injunctive, or other equitable relief.

204. Plaintiff and the Class members are entitled to punitive damages because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice.

205. Plaintiff and the Class members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

**COUNT V**
**Invasion of Privacy Under California's Constitution**
**(On Behalf of the California Subclass)**

206. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

207. Plaintiff brings this claim against Defendant individually and on behalf of the California Subclass.

208. Plaintiff and Class Members have an interest in: (1) precluding the dissemination of their sensitive, confidential online communications; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

209. At all relevant times, by using the Tracking Technologies to record and communicate their sensitive and confidential online communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

210. Plaintiff and Class Members had a reasonable expectation that their sensitive and confidential online communications, identities, and other data would remain confidential and that Defendant would not install wiretaps on the Website.

211. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' sensitive confidential online communications.

212. The invasion of privacy was serious in nature, scope, and impact because it related to their sensitive and private online communications. Moreover, it constituted an egregious breach of societal norms underlying the privacy right because Defendant promised to keep Plaintiff and Members of the California Subclass's communications confidential.

213. Accordingly, Plaintiff and members of the California Subclass seek all relief available for invasion of privacy claims under California's Constitution.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the putative Nationwide Class and California Subclass defined above, naming Plaintiff as the representative of the putative Classes, and naming Plaintiff's attorneys as Class Counsel to represent the putative Class and Subclass Members;

(b) For an order declaring that the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the putative Classes on all counts asserted herein;

(d) For statutory damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For injunctive relief as pleaded or as the Court may deem proper; and

(g) For an order awarding Plaintiff and the putative Classes their reasonable attorneys' fees and expenses and costs of suit.

## JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury for any and all issues in this action so triable of right.

Dated: July 2, 2026

Respectfully submitted,

**BURSOR & FISHER, P.A.**

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta (State Bar No. 354768)
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: (914) 874-0708
Facsimile: (914) 206-3656
Email: pfraietta@bursor.com

*Counsel for Plaintiff*