**IN THE UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF NEW YORK**

| | |
|---|---|
| ALESSANDRO DE LA TORRE and JOHN BAKER, individually and on behalf of all others similarly situated,<br><br>*Plaintiffs*,<br><br>v.<br><br>TABOOLA, INC., a Delaware corporation,<br><br>*Defendant*. | Case No. |

**CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiffs Alessandro De La Torre and John Baker bring this Class Action Complaint and Demand for Jury Trial on behalf of themselves and all others similarly situated against Taboola, Inc. for unlawfully intercepting users' online communications, using that data to build highly detailed, persistent "cradle-to-grave" consumer profiles, and disseminating their data to numerous third parties, including foreign adversaries, in violation of state and federal law and fundamental privacy rights. Plaintiffs allege as follows based on personal knowledge as to themselves and on information and belief as to all other matters.

**NATURE OF THE ACTION**

1. This case challenges Defendant Taboola's operation of a sweeping and nearly invisible "commercial surveillance" system targeting U.S. consumers.[1] Taboola runs one of the most pervasive and intrusive consumer surveillance operations on the internet: a platform that

[1] The Federal Trade Commission defines "commercial surveillance" as the business of collecting, analyzing, and profiting from information about people. *Commercial Surveillance and Data Security Rulemaking*, Fed. Trade Comm'n (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

silently tracks hundreds of millions of users across thousands of unrelated websites, intercepting the private browsing activity of millions of Americans, amassing details about their personal lives, and building rich individual-level behavioral profiles on each. Taboola aggressively monetizes these profiles, transmitting these sensitive details to numerous third parties for advertising, analytics, and related commercial purposes.

2. Plaintiffs and Class members never signed up for Taboola's services. They did not create Taboola accounts. They did not intend to communicate with Taboola. Most have never heard of Taboola. Yet Taboola intentionally acquires and exploits intimate information about unsuspecting consumers through hidden tracking code embedded in thousands of websites across the internet—code that activates the moment a page loads, before a user has read a single word or clicked a single link, and that operates entirely out of sight.

3. Taboola's commercial surveillance operates through a digital advertising system known as real-time bidding ("RTB"), an automated auction process in which advertisers compete in milliseconds to display their ads to specific users.[2] These auctions take place surreptitiously in the background each time a webpage loads.

4. Most internet users have encountered Taboola's products without realizing it. Its most recognizable format is the grid of thumbnail images and sensational headlines appearing beneath news articles on sites like Business Insider, The Daily Beast, and MSN, typically labeled "Recommended For You" or "Around the Web," with sponsored links like "Gut Doctor Begs Americans to Throw Out This Vegetable" interspersed among links to legitimate news stories.

[2] Roi Fainstein, *What is RTB? Real-Time Bidding Explained for Advertisers*, realize: Mktg. Hub (Apr. 20, 2022), https://www.taboola.com/marketing-hub/what-is-real-time-bidding/.

These so-called native content recommendation "widgets" are designed to mimic the look and feel of editorial content on the host site, blurring the line between journalism and advertising.

5. It works like this: as users browse sites embedded with Taboola's tracking code, Taboola intercepts detailed user data and merges it with existing user profiles linked to persistent, unique identifiers that Taboola has assigned to each consumer. These identifiers enable Taboola to recognize the same individuals across time, devices, and contexts, making such users identifiable, trackable, and targetable. Using these identifiers, Taboola aggregates information about a user's behavior across the internet into a single, unified profile. Taboola enriches these identifier-linked profiles with information obtained from third-party data brokers, identity vendors, and Taboola's own behavioral analysis.

6. Intimate, highly detailed inferences and observations are made about users based on their behavior, such as their health conditions, relationship status, occupation, financial condition, location, and sexual preferences. Through ongoing collection, retention, enrichment, and circulation of user data, Taboola creates and monetizes comprehensive "cradle-to-grave" user profiles that track individuals' behaviors, interests, and traits across large swaths of their digital lives.

7. The harm does not stop with the construction of these invasively detailed profiles. Taboola's real-time bidding system is designed to broadcast what is known as "bidstream data" to third parties participating in an advertising auction. Taboola packages what it knows about the user, including the individual's persistent identifiers, the specific webpage they are viewing, their device identifiers, IP address, browsing history, and inferred personal characteristics, into a data bundle called a "bid request." Taboola then broadcasts that bundle simultaneously to dozens or hundreds of potential advertisers. Those advertisers then bid for the right to show the user an ad.

Taboola will then display the advertiser's winning ad on the webpage. This is the engine of Taboola's business, repeated hundreds of millions of times each day across thousands of websites.

8. The entire process is invisible to the user and completes before the user can even see the fully loaded webpage. Critically, every third party anywhere in the world that receives a bid request gets the user's personal data, regardless of whether they win the auction. The universe of recipients is not limited to advertisers seeking to sell products. It includes data brokers, audience intelligence platforms, and other commercial entities whose core business is the collection, aggregation, and resale of personal information. There is no technical mechanism requiring losing bidders to discard what they received, meaning that these third parties are free to share, resell, or otherwise leverage this data, creating a cascading series of privacy violations.

9. Taboola's conduct also poses a serious threat to national security. As detailed below, Taboola transmits Americans' sensitive data to Chinese technology companies, including companies that the U.S. Department of Defense has formally identified as extensions of the Chinese military. These transmissions expose detailed information about Americans' health concerns, financial vulnerabilities, and personal circumstances to exploitation by a foreign adversary. And once broadcast through real-time bidding, that information can never be meaningfully recalled or secured.

10. Every page load on a Taboola-enabled website results in covert surveillance, and every ad auction in a mass disclosure of the collected data. The scale, intimacy, and opacity of this system represent a profound and ongoing violation of the reasonable expectation of privacy held by every American who uses the internet.

11. As detailed herein, Plaintiffs bring claims on behalf of two overlapping classes. First, Plaintiffs allege that on certain websites that deploy Taboola's tracking and identity-synchronization code, Taboola transmits users' data to Baidu, Inc. ("Baidu"), Tencent Holdings Ltd. ("Tencent"), and/or Temu, Chinese technology companies, in violation of federal restrictions on the transfer of Americans' bulk sensitive personal data to entities associated with foreign adversaries. Those users comprise the nationwide BSD Class, as defined below.

12. Second, Plaintiffs allege that Taboola operates a pervasive system that generates and disseminates consumer profiles for commercial gain; California residents subjected to that profiling comprise the California Class, as defined below.

13. Although the classes overlap, they are not coextensive, as the BSD Class is defined by unlawful transfers to Temu, Baidu, and Tencent, while the California Class is defined by privacy-violating profiling practices under California law.

14. Plaintiffs seek statutory and compensatory damages as well as equitable relief, including an injunction prohibiting Taboola from continuing to intercept user communications and from aggregating or transmitting sensitive user data to third parties in violation of federal and state law and fundamental privacy rights.

## PARTIES

15. Plaintiff Alessandro De La Torre is a natural person and citizen of the State of California.

16. Plaintiff John Baker is a natural person and citizen of the State of Illinois.

17. Defendant Taboola, Inc. is a corporation organized and existing under the laws of Delaware, with its principal place of business located at 16 Madison Square West, 7th Floor, New York, New York 10010.

## JURISDICTION AND VENUE

18. This Court has jurisdiction over this action (1) pursuant to 28 U.S.C. § 1331 because cases under the ECPA, 18 U.S.C. § 2510, et seq., raise a federal question and (2) pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because (i) at least one member of the Class is a citizen of a different state than any Defendant, (ii) there are more than 100 Class Members, (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (iv) none of the exceptions under that subsection apply to this action.

19. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District and is headquartered in this District.

20. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District.

## COMMON FACTUAL ALLEGATIONS

### I. Taboola's Scale and Reach in the Online Advertising Ecosystem.

#### a. Taboola's Presence on More Than 100,000 Websites Enables It to Intercept, Enrich, and Distribute User Data at Massive Scale.

21. Taboola operates one of the most pervasive and recognizable "content recommendation" and programmatic advertising platforms in the global digital advertising industry. Founded in 2007 and publicly traded on Nasdaq, Taboola reaches over 600 million daily active users across the globe. Its platform processes approximately 500,000 "recommendation-related" requests every second. Taboola technology appears on over 100,000 websites with major publishing partners, including NBCUniversal News Group, Yahoo, and Apple News.[3]

[3] News Release, *Taboola Announces New, Five-Year Deal with NBCUniversal News Group, Including NBC News, CNBC, MSNBC and Today*, Taboola (Nov. 28, 2023),

22. Programmatic advertising—sold through automated real-time bidding auctions—accounts for the vast majority of digital advertising in the United States, with industry estimates indicating that nearly 90% of digital ads are delivered through this model.[4,5] Taboola plays a dual role in this ecosystem, operating an exchange through which advertisers bid on ad inventory while simultaneously harvesting the behavioral data that makes that targeting possible.

23. As introduced above, Taboola's "content recommendation widgets"—the familiar grid of sponsored links and thumbnails appearing at the bottom of web pages under labels such as "Sponsored Content" or "You Might Also Like"—are embedded across thousands of high-traffic websites in the United States, including general news and entertainment sites as well as more sensitive websites focused on reproductive care, mental health, financial hardship, and other deeply personal topics.

24. While the widgets are Taboola's most recognizable format, Taboola serves advertisements in other formats through the same underlying infrastructure. Whatever the format, Taboola selects sponsored content tailored to each individual visitor in real time—

---

https://investors.taboola.com/news-releases/news-release-details/taboola-announces-new-five-year-deal-nbcuniversal-news-group; Marcus Mendes, *Apple dinged over low-quality, scammy-looking ads on Apple News*, 9to5Mac (Feb. 6, 2026), https://9to5mac.com/2026/02/06/apple-dinged-over-low-quality-scammy-looking-ads-on-apple-news/; Press Release, *Yahoo and Taboola Announce Closing of Deal, 30-Year Strategic Partnership Sees Taboola Power recommendations for Yahoo*, Taboola (Jan. 17, 2023), https://www.taboola.com/press-releases/taboola-and-yahoo-close-deal/.

[4] Programmatic advertising is the automated buying and selling of digital advertising space using software systems and real-time auctions, in which ads are selected and delivered to users based on data about the user, the content being viewed, and advertiser bidding criteria, typically within milliseconds of a webpage or app loading.

[5] Bill Nash, *Programmatic Advertising Statistics 2025: 91+ Stats & Insights,* Marketing LTB Blog, https://marketingltb.com/blog/statistics/programmatic-advertising-statistics/ (last visited July 24, 2026).

personalization that begins the moment a Taboola-enabled webpage loads, activating tracking technologies that extract user data before the page has even finished rendering.

25. Taboola promotes its platform by touting the scope of its data collection and the granularity of its targeting capabilities, and its Annual Report (Form 10-K), filed February 25, 2026, offers striking insights into the true scale of that operation. Taboola says its tracking and targeting capabilities are enhanced by its AI-powered "recommendation" engine, an AI system that leverages its access to "unique 'pulse of the internet' data"—real-time insight into what people read, buy, and do across its vast publisher network.

26. Taboola's systems handle 500,000 recommendation-related requests every second, and its platform has served up to 1.2 trillion recommendations in a single month. Each of those requests represents a moment when a real person loaded a real webpage, and Taboola's systems fired—intercepting that person's communications, consulting their accumulated behavioral profile, running a real-time auction among dozens of potential buyers, and selecting a targeted advertisement, all before the page finished loading.

27. While the number of targeted ads Taboola serves up is staggering, the colossal scale of the data collected, processed, and stored by Taboola is nearly impossible to grasp. Taboola operates approximately 14,000 servers across four back-end data centers and seven front-end global data centers. Those data centers together process more than 170 terabytes of data every single day—the equivalent of ingesting tens of millions of books' worth of information about user behavior every 24 hours. That daily intake feeds an AI engine that Taboola claims it has spent over fifteen years training on the browsing habits, content preferences, and inferred personal characteristics of hundreds of millions of people.

28. The cumulative result of that daily intake is a data stockpile of almost incomprehensible size. Taboola discloses that it maintains approximately 99,000 petabytes of storage, equivalent to 99,000,000,000 gigabytes.

29. To put that figure in perspective, the entire English-language text of Wikipedia requires around 24 gigabytes of storage. Taboola stores approximately 4.1 billion times that amount. This hoard is a testament to the scale of Taboola's surveillance, built one page view at a time from the private browsing behavior of hundreds of millions of people who never agreed to be watched.

**b. Taboola Intercepts Website Communications, Diverts Data to Its Own Servers, and Syncs User Identifiers with Third Parties to Enrich and Monetize Consumer Profiles.**

30. To power its advertising platform, Taboola provides publishers with invisible tracking and auction technologies that are embedded directly into publishers' websites.

31. These technologies execute automatically within users' browsers when a page loads, allowing Taboola to intercept, duplicate, and redirect data generated during users' electronic communications with websites.

32. Taboola's interception technologies include, among others:

a. JavaScript tracking scripts, which are embedded directly in the source code of partner websites and execute automatically when a page loads, causing the user's browser to transmit information about the user's session, device, and page activity to Taboola-controlled servers;

b. Tracking pixels, which are tiny, invisible files embedded within publisher webpages that fire automatically as the page loads, instructing the user's browser to transmit data about the user and the page being viewed to Taboola's servers; and

c. Identity-syncing endpoints, which instruct the user's browser—typically through HTTP redirects and cookie-based requests—to contact Taboola and third-party tracking domains to exchange identifiers so that multiple advertising technology companies can recognize and track the same user across websites, sessions, and devices.

33. When a user visits a website incorporating Taboola's tracking infrastructure, Taboola's code executes contemporaneously with the user's communication with the website. Information intended for the first-party website—such as requests for page content—is duplicated and redirected to Taboola's servers as part of the same rendering sequence, without the user's knowledge or consent, before the user can even interact with the still-loading webpage.

34. The data transmitted to Taboola includes the user's IP address, browser and operating system details, device and cookie identifiers, the full URL of the page being visited (including query strings and URL parameters), and the referring URL. Together, these signals reveal the precise content the user is viewing at the moment of interception—regardless of how sensitive that content may be. The full URLs also allow Taboola to attach content classifications and audience segments to the data before transmitting it to potential ad buyers.

35. Taboola then uses the intercepted data for profiling and targeting. As described below, Taboola assigns users to behavioral categories, links their identities across devices and platforms, and broadcasts details about their lives to third-party advertisers and data brokers, including entities operating under the laws of foreign adversaries.

## II. Taboola's Construction of Persistent Consumer Profiles.

### a. Taboola's Persistent Identifier System Enables Long-Term Individual Tracking Across the Internet Despite Claims of Pseudonymity.

36. Central to Taboola's surveillance infrastructure is a persistent user identifier: a unique sequence of letters and numbers stored in a cookie on the user's device and continuously

refreshed by Taboola with each new interaction.[6] This identifier, which Taboola's documentation identifies as the "t_gid" (hereinafter, the "Taboola ID"), is set on the user's device by Taboola's servers.

37. The Taboola ID functions as a permanent tracking number assigned to the user, enabling Taboola to recognize the same individual across thousands of websites, across months and years of browsing activity, and across the entirety of Taboola's publisher network. The same Taboola ID that Taboola reads when a user visits a financial news website in the morning is the identifier it reads when that user visits a chronic illness support site in the afternoon, allowing Taboola to link those seemingly independent visits into a single profile of that user's activity. That identifier is not separate from the user. It is the user, for all practical purposes of tracking, targeting, and profiling.

38. Taboola attempts to reassure consumers and investors that it collects only "pseudonymized" data, claiming that because it does not collect information like users' names or email addresses, it cannot know who its users are. That characterization is at best incomplete and at worst deliberately misleading. As described below, it is also contradicted by the technical realities of Taboola's operations and by Taboola's own public statements.

39. Regulatory authorities have made clear that identifiers like the Taboola ID are not meaningfully anonymous or pseudonymous merely because they lack obvious personal labels. The Federal Trade Commission ("FTC") has explained that, "[r]egardless of what they look like, all user identifiers have the powerful capability to identify and track people over time, therefore the **opacity of an identifier cannot be an excuse for improper use or disclosure**." (emphasis

[6] A "cookie" is a small text file that web services can place on a user's device to retain information about that user.

in original).[7] The FTC has further stated that "[c]ompanies 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."[8]

40. Taboola actively and deliberately links its internal identifiers to identifiers held by dozens of third-party data brokers, advertisers, and demand-side platforms—some of which possess users' names, email addresses, purchase histories, physical addresses, and other directly identifying information. The moment the Taboola ID is linked to a partner's identifier that is itself tied to a real identity, any pseudonymity is gone—not just for that partner, but for the entire ecosystem of entities that can cross-reference the synchronized identifiers.

41. Even absent a link to a name or email address, the data Taboola collects is identifying. Taboola's own materials acknowledge the risks of collecting what it calls "indirect" personally identifiable information or "quasi-identifiers," such as IP addresses, device IDs, browser fingerprints, demographic information, and geolocation: "There are numerous ways indirect [personally identifiable information] can become identifiable when cross-referenced with other pieces of information. For instance, an IP address coupled with an individual's browsing history, device ID, and/or ad interactions can reveal a user's identity."[9] By Taboola's own admission, the very identifiers it passes off as innocuous are capable of revealing an individual's real-world identity.

---

[7] *No, hashing still doesn't make your data anonymous*, Fed. Trade Comm'n Tech. Blog (July 24, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

[8] *Id.*

[9] Jennifer Lobb, *Personally Identifiable Information (PII): Leveraging Personalization with Care*, realize: Mktg. Hub (July 10, 2025), https://www.taboola.com/marketing-hub/personally-identifiable-information/.

42. Taboola's published materials go further, acknowledging that re-identification is straightforward: "The ability to associate multiple pieces of indirect [personally identifiable information] to establish an individual's identity is becoming increasingly easy, thanks to advanced algorithms and data brokers that use this data to create user profiles. As such, what is often considered anonymous data can become personally identifiable when aggregated."[10]

43. Taboola is one such data broker—registered as such with the State of California—and it is directly and intentionally integrated with more than a dozen data brokers that are similarly registered. Taboola has engineered its infrastructure specifically to facilitate the exchange of persistent identifiers and the aggregation of personal information across this network.

44. Taboola's pseudonymity claims thus collapse under the weight of its own admissions. Taboola knows how re-identification works, and it knows that the data points it collects and shares are, in combination, sufficient to identify a real person. A company that publicly states that anonymous data becomes personally identifying when aggregated cannot credibly claim that its own aggregation of that same data is harmless.

**b. Taboola Builds Consumer Profiles Through Direct Data Collection, Content Engagement Signals, and Third-Party Data Partner Relationships.**

**i. Taboola Collects Browsing Activity and Generates Behavioral Inferences to Populate Individual Consumer Profiles.**

45. Taboola uses the data it collects to generate behavioral, demographic, and intent-based profiles of each user. It assigns consumers to audience "segments"—predefined categories that advertisers can target directly through Taboola's platform. These segments are built from a

[10] *Id.*

user's browsing behavior across Taboola's vast publisher network and are designed to predict personal traits, needs, and vulnerabilities.

46. Examples of the classifications Taboola assigns to users include "Expectant Mothers / Pregnancy," "I Frequently Take Preventative Medicine," "Minimum Payment on Credit Card Debt," "Smart Investor: Far Below Average," and "LGBT Donor." Each segment is linked to the user's persistent identifiers, so these classifications follow the individual across websites, sessions, and devices—and the profile deepens with every page view.

47. Taboola's segmentation capabilities are extensive. Through its AI-driven recommendation engine and its network of data partners, Taboola builds profiles encompassing a wide range of personal characteristics—including inferred health conditions, financial circumstances, political orientation, religious beliefs, sexual orientation, and other sensitive attributes. As described in the next section, Taboola does not build these profiles from its own data collection alone; it enriches them with data acquired from third parties.

#### ii. Taboola Enriches Profiles by Exchanging Persistent Identifiers with Third-Party Data Brokers and Advertising Partners.

48. The behavioral profiles Taboola builds through its own data collection are only a starting point. To deepen those profiles and increase their commercial value, Taboola synchronizes its user identifiers with third-party data brokers, advertising platforms, and other partners—expanding both what is known about each user and who knows it.

49. This process, known as "identity syncing" or "cookie syncing," works as follows: Taboola instructs the user's browser to contact a third party's servers, passing the user's Taboola ID in the outbound request. The third party can then associate its own identifier for that user with Taboola's, allowing both companies to recognize and track the same individual and to share data about them across platforms.

50. Taboola partners with dozens of entities throughout the digital advertising space, ranging from domestic data brokers like LiveRamp to Chinese technology companies like Baidu, Tencent, and Temu. Through identity syncing with partners like these, Taboola enables the cross-referencing of its internal user profiles with profiles maintained independently by third-party data brokers and advertisers.

51. This process allows Taboola and its downstream partners to build and continuously update comprehensive behavioral dossiers on individual users, tying together browsing activity, demographic information, purchase history, and other sensitive attributes sourced from multiple independent data streams. Whatever Taboola may claim about the "pseudonymity" of its data, the result is that each user is in practice identifiable and trackable by a broad network of commercial entities, including by Taboola itself.

**iii. Taboola Uses Real-Time Bidding to Continuously Expand and Redistribute Consumer Profiles to a Global Network of Third Parties.**

52. When an open ad placement becomes available within a Taboola advertising slot on a publisher's website, Taboola may fill it by soliciting real-time bids from external advertisers and demand-side advertising platforms. In this process, Taboola packages the user's behavioral and contextual profile into a bid request, which it broadcasts to prospective bidders—including entities subject to the jurisdiction and control of foreign adversaries of the United States.

53. Each bid request transmitted by Taboola includes a rich set of personal data, including, on information and belief: the full URL of the page being viewed, the user's inferred audience segments, persistent identifiers, IP address, browser and operating system details, and contextual classifications of the content being consumed. This data is transmitted to all eligible bidders simultaneously, not only to the single ultimate winner of the auction.

54. Although only one advertiser wins any given auction, on information and belief, every recipient of the bid request receives persistent identifiers, IP addresses, device and browser information, the specific webpage or application being accessed, and inferred demographic or behavioral attributes. This means that dozens or hundreds of third-party recipients receive detailed information about each user's browsing activity, interests, and inferred characteristics with each page view—regardless of whether that third party ultimately displays an ad to that user.

55. There are no technical limitations in the RTB process that prevent recipients from retaining, aggregating, or repurposing this data beyond the immediate auction, and many do so. Third parties can siphon off Taboola's bidstream data at massive scale and use it to build their own independent consumer dossiers—often without any direct relationship to the user and without meaningful oversight.

56. The consequences of this data exposure cascade well beyond the advertising transaction. With each ad auction, new behavioral signals are attached to existing profiles—not just by Taboola, but also by the numerous third parties who receive the bid requests. These profiles can be enriched over time by correlating bidstream data received from multiple ad exchanges and publishers, allowing recipients to reconstruct detailed histories of individuals' online behavior, interests, locations, and vulnerabilities. This creates a self-reinforcing cycle of redisclosure, wherein increasingly comprehensive identity dossiers are built and shared over time, continuously enriched by new behavioral signals drawn from across the web.

57. The risks posed by RTB systems to Americans' privacy and national security are not new, and they are not unknown. They have been expressly and publicly identified by Congress. In April 2021, a bipartisan group of United States Senators—including Senators Bill

Cassidy, Ron Wyden, Kirsten Gillibrand, Mark Warner, Sherrod Brown, and Elizabeth Warren—sent formal letters to major digital advertising exchanges warning about the national security implications of RTB systems.[11]

58. The Senators warned that "[f]ew Americans realize that some auction participants are siphoning off and storing 'bidstream' data to compile exhaustive dossiers about them[,]" and that these dossiers were "being openly sold to anyone with a credit card, including to hedge funds, political campaigns, and even to governments." (internal quotations omitted). *Id.* They emphasized that RTB systems routinely distribute sensitive information—including device identifiers, cookies, browsing and location data, IP addresses, and demographic attributes—to large numbers of auction participants with no meaningful ability to control downstream use.

59. The Senators further warned that this data would be "a goldmine for foreign intelligence services[,]" capable of being exploited to "supercharge hacking, blackmail, and influence campaigns." *Id.* They explained that the national security threat arises precisely because RTB systems broadcast sensitive user data to numerous third parties simultaneously, with limited transparency and no technical mechanism to prevent secondary use, retention, or resale.

## III. Taboola's Identity Synchronization with Chinese Companies Results in Dangerous and Ongoing Transfers of Americans' Sensitive Data in Violation of Federal Law.

### a. Taboola Actively Synchronizes Persistent Identifiers with Chinese Companies That the Pentagon Has Identified as Instruments of the Chinese Military.

60. As part of its real-time bidding operations, Taboola maintains active identity

[11] Press Releases, *CASSIDY, BIPARTISAN SENATORS QUESTION ONLINE AD EXCHANGES ON SHARING AMERICAN'S DATA WITH FOREIGN COMPANIES*, Bill Cassidy U.S. Sen. for La. (Apr. 5, 2021), https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-bipartisan-senators-question-online-ad-exchanges-on-sharing-americans-data-with-foreign-companies/.

synchronization integrations that permit the exchange of persistent identifiers with multiple Chinese technology companies. At least two of those companies—Baidu, Inc. and Tencent—have been identified by the U.S. Department of Defense as Chinese military companies operating in the United States.

61. Baidu, Inc. is a sprawling Chinese technology company headquartered in Beijing. Founded in 2000, Baidu specializes in internet services and artificial intelligence. Its core business is online search, where it holds a dominant position in China's search engine market, with online marketing as a key source of revenue. Beyond search, Baidu operates a range of consumer internet services spanning content and information platforms, online encyclopedic and forum communities, video streaming, mapping, and cloud storage. The company has also diversified substantially into artificial intelligence, building a full-stack business that includes foundation models, generative AI chatbots, deep learning platforms, cloud infrastructure, and semiconductor design.

62. Tencent is a Chinese technology conglomerate and holding company headquartered in Shenzhen. Founded in 1998, Tencent now ranks among the world's largest companies by revenue and market capitalization. Its operations span several core business segments, including video gaming, fintech, cloud computing, social media, and, critically for purposes of this action, digital advertising. Tencent also invests substantially in areas such as artificial intelligence and holds minority stakes in hundreds of companies worldwide.

63. The problem with sharing Americans' data with these companies is not their foreign ownership; it is their obligations to the Chinese state. The U.S. Department of State has described the PRC's national development strategy as one of "Military-Civil Fusion," a deliberate and compulsory dissolution of the barriers between China's civilian commercial

enterprises and its military and defense industrial sectors.[12] Under this strategy, ostensibly private technology companies serve as instruments of state and China's burgeoning military power.

64. Baidu and Tencent have each been directly identified as just such instruments. Pursuant to Section 1260H of the National Defense Authorization Act for Fiscal Year 2021, the U.S. Department of Defense maintains a regularly updated list of "Chinese Military Companies" operating in the United States (the "1260H List"). Inclusion on the 1260H List is a public statement by the Pentagon that it regards the listed company as functioning as an extension of the PRC's military apparatus.

65. The 1260H List captures a wide cross-section of China's economic operations, spanning technology companies of every kind, from component manufacturers to biotechnology firms to robotics companies. Tencent was added to the 1260H List in 2025.[13] In 2026, Baidu was added.[14]

66. The presence of both Tencent and Baidu on the 1260H List underscores the gravity of what is alleged here. When Taboola synchronizes persistent identifiers and exchanges data with these companies, it is not merely sharing information with foreign commercial actors. It is channeling bulk sensitive data concerning United States citizens to entities that the United

[12] *Military-Civil Fusion and the People's Republic of China*, U.S. Dep't of State, https://2017-2021.state.gov/wp-content/uploads/2020/06/What-is-MCF-One-Pager.pdf (last visited July 23, 2026).

[13] https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF (last visited July 23, 2026).

[14] https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF (last visited July 23, 2026).

States government has formally identified as extensions of the Chinese military, posing a profound danger to both individual privacy and national security.

**b. Taboola Actively Synchronizes Persistent Identifiers With Temu, Another Chinese Company Subject to the Jurisdiction and Control of the Chinese Communist Party.**

67. Temu is a Chinese e-commerce company owned by PDD Holdings, Inc. Temu launched its U.S. operations in September 2022 and has since become the subject of widespread concern from U.S. government officials, law enforcement agencies, and national security experts regarding its invasive data collection practices and ties to the Chinese Communist Party ("CCP").

68. In September 2024, Congressional Republicans on the House Permanent Select Committee on Intelligence formally requested briefings from the Federal Bureau of Investigation ("FBI") and Securities and Exchange Commission regarding Temu and its parent company. The members stated that they were "concerned about the protection of Americans' data" and emphasized that, "[a]nalogous to Congress' action on TikTok, the relationship between the Chinese Communist Party, Chinese national security laws, and Americans data must be understood[,]" further expressing concerns that the CCP may be attempting to exploit U.S. democratic institutions, free-market principles, and the personal and economic data of Americans.[15]

[15] Press Release, *LAHOOD, HPSCI REPUBLICANS SOUND ALARM ON TEMU, REQUEST BRIEFING FROM FBI AND SEC*, House Permanent Select Comm. on Intel. (Sept. 25, 2024), https://intelligence.house.gov/2024/09/25/lahood-hpsci-republicans-sound-alarm-on-temu-request-briefing-from-fbi-and-sec/.

69. In April 2024, multiple U.S. Senators wrote to President Biden about Temu's dangerous conduct.[16] U.S. Senator Tom Cotton argued that urgent action was needed to "protect every single American's personal privacy" from Temu's practice of "harvesting vast amounts of personal information from American consumers" and its ties to the CCP.[17] Around the same time, Congressman Brian Mast urged the FTC to investigate Temu's connections to the CCP.[18]

70. In August 2024, Senator Rick Scott wrote to Secretary of Commerce Gina Raimondo urging the Department of Commerce to investigate the "CCP-linked" Temu, expressing serious concerns about data privacy, in addition to labor practices and product safety.[19] That same month, Attorneys General from twenty-one states sent a joint letter to Temu's president and PDD Holdings' CEO demanding that Temu disclose how it collects and stores consumer data and whether it sells that data to third parties.[20]

71. Multiple independent analyses have confirmed the invasive nature of Temu's data collection practices. For example, in October 2024, the Center for Strategic and International

---

[16] Elaine Mallon & Washington Examiner, *GOP senators call on Biden administration to investigate popular Chinese marketplace websites*, Denver Gazette (Apr. 17, 2024), https://www.denvergazette.com/2024/04/17/gop-senators-call-on-biden-administration-to-investigate-popular-chinese-marketplace-websites-3354c847-f87c-5870-9c58-9dbf9ec96428/.

[17] Letter from Sen. Tom Cotton to President Joseph R. Biden, U.S. Senate (Apr. 15, 2024), https://www.nationalreview.com/wp-content/uploads/2024/04/temu_letter.pdf.

[18] Office of Rep. Brian Mast, *Mast Demands FTC Probe Temu for Alleged Ties to the CCP* (Apr. 17, 2024), https://mast.house.gov/2024/4/mast-demands-ftc-to-probe-temu-for-its-alleged-ties-to-ccp.

[19] Press Release, Sen. Rick Scott, *Sen. Rick Scott Urges Department of Commerce to Investigate CCP-Linked Temu* (Aug. 14, 2024), https://www.rickscott.senate.gov/2024/8/sen-rick-scott-urges-department-of-commerce-to-investigate-ccp-linked-temu.

[20] Letter from Att'ys Gen. of 21 States to Qin Sun (Temu) and Chen Lei (PDD Holdings) (Aug. 15, 2024), https://www.tn.gov/content/dam/tn/attorneygeneral/documents/pr/2024/temu-letter.pdf.

Studies issued a report highlighting Temu's concerning data collection practices and its legal obligation to cooperate with Chinese intelligence agencies.[21]

72. In July 2025, Kentucky Attorney General Russell Coleman filed a lawsuit against Temu, alleging that Temu illegally provides the Chinese government with access to Americans' data.[22] Since June 2024, the Attorneys General of at least seven states—Arizona, Arkansas, Iowa, Kentucky, Nebraska, Oklahoma, and Texas—have filed similar lawsuits alleging, among other things, that Temu's mobile app functions as spyware designed to harvest Americans' personal information.

73. Despite the widely recognized national security risks posed by Temu and its documented data-collection practices, Taboola has knowingly maintained active technical integrations with Temu that enable the systematic transfer of Americans' persistent identifiers and related data through identity synchronization.

**c. Taboola's Identity Synchronization Enables Baidu, Tencent, and Temu to Track Millions of Americans Across the Internet.**

74. Taboola's integration with Baidu, Tencent, and Temu is not an accident; all three are listed in Taboola's own public roster of "RTB Partners." As part of Taboola's integration with each of these companies, Taboola's code causes users' browsers to silently exchange identifiers with that partner's servers, sending the Taboola ID for the user and receiving the partner's corresponding internal identifier in return. The mechanism described below operates identically for Baidu, Tencent, and Temu.

---

[21] Diane Rinaldo, *Looking Beyond TikTok: The Risks of Temu*, Center for Strategic and International Studies (Oct. 2024), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-10/241023_Rinaldo_Temu_Brief.pdf?VersionId=YHKZ_M7RQpFKe6Cy1hMeZ4OfCaJ9Nuyp.

[22] Kevin Grout, *Attorney General Coleman Files Lawsuit Against Chinese Shopping Platform Temu for Stealing Kentuckians' Data*, Kentucky Attorney General (July 17, 2025), https://www.kentucky.gov/Pages/Activity-stream.aspx?n=AttorneyGeneral&prId=1797.

75. Before the first time this exchange takes place, Taboola and the partner might each know the same user by completely different identifiers. In other words, the two companies could be looking at the same individual but would not know it because each is using its own private labeling system.

76. Identity synchronization solves this problem for the companies. Taboola instructs the user's browser to contact the partner's server and to bring Taboola's user identifier along with it. The browser does just that, automatically and invisibly, delivering that user's unique Taboola ID and other data like the user's IP address directly to the partner's server.

77. When the partner receives that information, it records Taboola's identifier along with its own internal identifier for that user, marking down that both identifiers belong to the same individual. From that point on, whenever the partner encounters either identifier in any context, it knows that they refer to the same person. This means the partner is now able to cross-reference everything it already knows about that user from its own advertising platform with everything it receives from Taboola's RTB activity going forward. This process essentially merges two previously siloed surveillance profiles into one single, even richer profile that persists indefinitely.

78. Put differently, through this identity synchronization process, each partner receives persistent identifiers tied to American users, along with associated IP addresses and other technical metadata, and links that information to its own internal user profiles. This creates a persistent linkage that allows the partner to recognize and track the same individual across the RTB advertising ecosystem and across unrelated websites and digital contexts.

79. This linkage does not expire with a single session. Because both Taboola's and the partner's identifiers are stored as long-lived cookies on the user's device, the synchronized

relationship persists for months or years, enabling the partner to build a continuously expanding profile of the user's browsing activity across Taboola's entire publisher network.

80. More troubling still, once a partner has synchronized identifiers with Taboola, it can correlate that identifier linkage with bidstream data it receives from other participants in the RTB system.

81. In the RTB ecosystem, dozens of advertising platforms routinely broadcast bid requests containing persistent identifiers, URLs, and behavioral segment data. Using the synchronized identifiers as a common key, Baidu, Tencent, and Temu can each match and aggregate this information across multiple sources. This allows each of them to piece together comprehensive profiles of American consumers' browsing behavior, interests, health concerns, and inferred characteristics, even when these users have never visited that company's website or knowingly interacted with its services.

82. Taboola's transmission of persistent identifiers and IP addresses to these companies is prohibited by federal national security law, as explained below.

**d. The BSD Rule Prohibits Taboola's Transmission of Americans' Persistent Identifiers to CCP-Linked Entities Like Baidu, Tencent, and Temu.**

83. On April 8, 2025, the U.S. Department of Justice issued the BSD Rule, codified at 28 C.F.R. Part 202, to restrict the transfer of Americans' bulk sensitive personal data to "countries of concern"—including the People's Republic of China. The BSD Rule was promulgated pursuant to Executive Order 14117, which identified the unrestricted transfer of Americans' personal data to foreign adversaries as a national security threat.

84. Under the BSD Rule, it is unlawful to engage in any "covered data transaction" that involves the transfer of "bulk U.S. sensitive personal data" or "bulk covered personal identifiers" to entities that are owned by, controlled by, subject to the jurisdiction of, or

organized under the laws of a country of concern. 28 C.F.R. §§ 202.206, 202.210, 202.212. The rule applies specifically to transactions involving data brokerage and online advertising, the exact activities in which Taboola engages.

85. The U.S. government has determined that the export of Americans' behavioral data to hostile foreign regimes or entities under their jurisdiction constitutes an "'unusual and extraordinary threat . . . to the national security and foreign policy of the United States' that has been repeatedly recognized across political parties and by all three branches of government."[23]

86. The BSD Rule defines "covered personal identifiers" to include persistent identifiers such as advertising IDs, device identifiers, and IP addresses. The Rule establishes "bulk" thresholds that trigger liability: transfers involving data linked to more than 100,000 U.S. persons over a twelve-month period constitute prohibited bulk transfers. 28 C.F.R. §§ 202.205, 202.211.

87. The BSD Rule provides examples of prohibited conduct that directly parallel Taboola's practices. One example describes a scenario in which a U.S. company that sells advertising space provides IP addresses and advertising identifiers associated with more than 100,000 U.S. persons to an advertising exchange located in a country of concern over a twelve-month period. 28 C.F.R. § 202.214(b)(4). The rule explains that this constitutes a covered data transaction involving data brokerage and is unlawful because IP addresses and advertising identifiers, when transferred in bulk, qualify as bulk covered personal identifiers.

[23] Press Release, *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries*, U.S. Dep't of Just. (Apr. 11, 2025), https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive.

88. That is precisely what Taboola does. By facilitating identity synchronization during its RTB activity, Taboola initiates the transmission of data packets that include U.S. users' persistent advertising identifiers—specifically, the Taboola ID—and IP addresses to Chinese companies including Baidu, Tencent, and Temu, entities operating under the jurisdiction of the People's Republic of China. These transmissions occur regularly, at massive scale, affecting millions of American users and vastly exceeding the BSD Rule's 100,000-person bulk threshold.

**e. Taboola's Ongoing Data Transfers Enable Foreign Surveillance, Exploitation, and Coercive Influence Over Americans.**

89. The danger addressed by the BSD Rule is not hypothetical or speculative. When persistent identifiers and detailed behavioral data are transferred in bulk to entities subject to the jurisdiction of a foreign adversary, those entities can aggregate the data into detailed dossiers about U.S. residents. Such dossiers can reveal individuals' health conditions, financial vulnerabilities, personal relationships, political views, physical locations, and psychological characteristics over time.

90. In the hands of an adversarial foreign government or its proxies, this information can be weaponized to identify and exploit individual Americans. Foreign intelligence services can use behavioral profiles to:

a. Identify Americans in sensitive positions—such as government employees, military personnel, intelligence officers, judges, law enforcement officials, or corporate executives—based on their online activity, location patterns, and institutional affiliations;

b. Target individuals for coercion, blackmail, or influence operations by identifying personal vulnerabilities such as financial distress, health conditions, addictions, or behavioral patterns that could be exploited;

c. Conduct surveillance of specific populations, including political activists, journalists, dissidents, human rights advocates, or members of diaspora communities who may be critical of the Chinese government; and

d. Build predictive models of American consumer behavior, political sentiment, public health trends, and social movements that can inform strategic decision-making by foreign governments seeking to undermine U.S. interests.

91. It is precisely this capacity to transform bulk advertising data into tools for surveillance, exploitation, and coercive influence that the BSD Rule was enacted to prevent—and that Taboola's continued transmissions to Baidu, Tencent, and Temu directly enable.

92. Taboola has knowingly continued routing Americans' sensitive user data to Baidu, Tencent, and Temu even after the BSD Rule took effect on April 8, 2025, even after Baidu's and Tencent's appearances on the Pentagon's 1260H List, and after widespread public reporting, congressional investigations, and state lawsuits documenting Temu's national security risks and invasive data practices.

**f. Taboola Knowingly Engaged in Prohibited Data Transfers Despite Clear Warnings.**

93. Taboola is not a passive or uninformed participant in the digital advertising ecosystem. It is a member of multiple industry groups—including the Network Advertising Initiative ("NAI")—that actively participated in the rulemaking process leading to the U.S. Department of Justice's adoption of the BSD Rule. In public comment letters submitted to DOJ during the rulemaking period, these trade associations specifically warned that certain advertising technology practices, such as behavioral profiling, identity syncing, and real-time

bidding with foreign demand-side platforms, could violate the BSD Rule if data was transmitted to entities linked to foreign adversaries like China.

94. Taboola's awareness of the legal risk posed by its data practices is further confirmed by its own SEC filings. In its Annual Report (Form 10-K), filed February 25, 2026, Taboola warned investors that "[o]ur ability to collect, augment, analyze, use, share and otherwise process data relies upon the ability to uniquely identify devices across websites, and applications, and to collect data about user interactions with those devices[.]"

95. Taboola's filing further acknowledges that it "collect[s] and store[s] IP addresses, cookie IDs, and other device identifiers that are or may be considered personal data in some jurisdictions or otherwise may be the subject of legislation or regulation" and that evolving definitions of personal data in the U.S. and abroad could "cause us to change our business practices[.]"

96. Despite clear guidance from the Department of Justice, prominent action by the Department of Defense, and widespread warnings from U.S. government officials and law enforcement, Taboola has continued to transmit sensitive user data to all three of these companies. By maintaining active identity synchronization integrations with Baidu, Tencent, and Temu—companies that have all been identified as threats to national security—Taboola has knowingly facilitated the export of Americans' behavioral data to a foreign adversary.

97. In doing so, Taboola has disregarded regulations enacted specifically to address what the U.S. government has called an "unusual and extraordinary threat" to the national security and foreign policy of the United States.[24]

[24] Press Release, *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries*, U.S. Dep't of Just. (Apr. 11, 2025),

## IV. Consumers Lack Notice, Choice, or the Ability to Consent to Taboola's Surveillance and Data Transfers.

98. Consumers have never heard of Taboola, have no relationship with Taboola, and have no meaningful way of knowing when Taboola is intercepting their communications. When visiting websites, users see only the publisher's domain and content. Taboola's presence is invisible, concealed in background code that executes automatically without any user-facing indication. Taboola's widgets are designed to appear as a feature of the publisher's website, not a gateway through which a third-party intermediary is surveilling, extracting, and monetizing intimate personal data in real time.

99. Even if a consumer somehow learned of Taboola's existence and sought to understand its data practices or exercise privacy rights, meaningful opt-out has been made functionally difficult. Taboola's privacy-related disclosures are dispersed across multiple policy documents hosted on its own domain, are not presented to users at the point of data collection, and provide no clear or accessible mechanism for users to prevent the real-time transmission of their data to hundreds of third-party partners during the RTB process.

100. Once Taboola broadcasts sensitive user data through its RTB system to countless third-party recipients, neither Taboola nor the user has any real ability to recall that data or prevent downstream misuse. This leaves users' sensitive data to be abused, resold, or repurposed indefinitely. The risk to users only increases when their information is made available in bulk to third parties looking to exploit sensitive user data, or to entities lacking adequate safeguards or internal controls.

---

https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive (internal quotation omitted).

101. Users who visit websites to research serious medical conditions, seek mental-health or addiction support, explore reproductive-health decisions, or engage in political organizing reasonably expect to communicate with the site they chose. They do not expect to have those communications silently intercepted and monetized by a silent and unknown surveillance intermediary that broadcasts detailed dossiers about their health status, beliefs, and personal vulnerabilities to an open marketplace of bidders, including foreign-adversary-controlled entities.

102. By concealing its surveillance, Taboola deprives users of any informed choice. Users are unaware that their sensitive browsing behavior is being intercepted, profiled, and transmitted through real-time auctions to dozens or hundreds of third parties with each page view, and they have no practical ability to avoid Taboola's surveillance while engaging in ordinary internet use.

103. This lack of visibility, transparency, and meaningful control is incompatible with widely recognized principles of privacy and data protection and is fundamentally at odds with consumers' reasonable expectations of privacy.

## FACTS SPECIFIC TO PLAINTIFF DE LA TORRE

104. Plaintiff Alessandro De La Torre is a resident of California who routinely uses the internet to conduct ordinary activities of daily life, including reading news, managing personal affairs, and researching topics of personal concern. Like the vast majority of Taboola's surveillance targets, Plaintiff De La Torre has never created an account with Taboola, and has never consented to Taboola's collection, profiling, or dissemination of his personal information.

105. In June 2025, while in California, Plaintiff De La Torre visited the regional news website HindustanTimes.com. Unknown to Plaintiff De La Torre, Taboola's code is deployed on

HindustanTimes.com and has been designed by Taboola to collect and share the personal information and browsing data of the website's users with numerous third parties.

106. While Plaintiff De La Torre was actively viewing pages on HindustanTimes.com, his browser loaded Taboola's JavaScript code, which was embedded on the site. This code executed silently and automatically during the page-load process, without any additional action by Plaintiff De La Torre. Taboola's code triggered an identity sync to de-anonymize Plaintiff De La Torre's data across multiple identity providers, enhancing the ability of Taboola and other third parties to recognize and track Plaintiff De La Torre across the internet on an ongoing basis. Plaintiff De La Torre's identity was synchronized at least three different Chinese technology companies associated with the CCP: Temu, Baidu, and Tencent.

107. On information and belief, Taboola initiated bid requests featuring persistent identifiers uniquely associated with Plaintiff De La Torre along with the full URL of the specific page that Plaintiff De La Torre was viewing on HindustanTimes.com at that time.

108. On information and belief, Taboola then enriched these bid requests with other data before sending the data to purchasers of ad inventory. Bid requests of this form routinely include behavioral segment data, which would further indicate and reveal Plaintiff De La Torre's interests and personal characteristics, even beyond what is revealed by the URL itself.

109. On information and belief, these segments, together with page-level context, were broadcast to dozens of advertising technology companies participating in the real-time bidding auction, resulting in these companies receiving detailed information about Plaintiff De La Torre's online behavior and interests in real time, without his knowledge or consent.

110. In March 2026, while in California, Plaintiff De La Torre visited TurboTax.Intuit.com, a website offering tax preparation services and advice. Unknown to

Plaintiff De La Torre, Taboola's code is deployed on the site and has been designed by Taboola to collect and share the personal information and browsing data of users with numerous parties and to intercept users' communications with the website. Plaintiff De La Torre was one such user. His information was intercepted, combined with other data, and shared without his permission.

111. While Plaintiff De La Torre was actively viewing pages on TurboTax.Intuit.com, his browser loaded Taboola's JavaScript code, which was embedded on the site. Taboola's code initiated a tracking request from Plaintiff De La Torre's browser to Taboola's servers. This code executed silently and automatically during the page-load process, without any additional action by Plaintiff De La Torre. This execution occurred as part of Taboola's effort to monetize his profile.

112. On information and belief, these Taboola-initiated requests featured persistent identifiers uniquely associated with Plaintiff De La Torre, including his cookie IDs, device IDs, IP address, and browser metadata, along with the full URL of the specific page that Plaintiff De La Torre was viewing at the time.

113. In April 2026, Plaintiff De La Torre submitted a data subject access request to Taboola to determine what information Taboola had collected and maintained about him. In response, Taboola disclosed a file revealing it had assigned Plaintiff a persistent tracking identifier—the Taboola ID (t_gid)—and had used that identifier to accumulate, assign, and make available to third parties thousands of audience segment classifications describing his personal characteristics, health status, financial condition, political beliefs, and military affiliation. Taboola maintains and shares these classifications with countless third parties, regardless of their veracity.

114. Taboola's dossier on Plaintiff De La Torre demonstrates that Taboola has made him available for targeting under at least the following sensitive categories:

115. Health. Taboola's records reveal that Plaintiff De La Torre has been assigned a segment originating from Swoop, a health data company that constructs propensity models from medical and behavioral data: specifically, segment swp_likely_73_t1d_propensity_nodx_092123_cln, which targets individuals that Swoop's model predicts are likely to have Type 1 diabetes but who have not received a formal diagnosis. Taboola made this classification available to advertisers through its RTB platform, broadcasting what amounts to a prediction of an undiagnosed chronic illness to an open marketplace of commercial bidders. Plaintiff De La Torre was not aware that this inference had been made about him, had not disclosed any such condition to Taboola or its partners, and did not consent to Taboola monetizing a prediction about his medical status.

116. Military and National Security Affiliation. Taboola's records show that Plaintiff De La Torre has been placed into at least three distinct segments related to military status or national security affiliation. These include an Experian segment labeled "Military > Active > Precision," which purports to identify individuals currently serving in the military, as well as a LiveRamp segment reflecting that Plaintiff De La Torre's inferred military status has been coded as "Retired," and an Eyeota segment classifying him under "Government Industry > National Security and International Affairs." These classifications are capable of exposing the military or national security status of a private individual to the open advertising marketplace, including to foreign adversary-affiliated entities such as Baidu, Tencent, and Temu.

117. Financial Vulnerability. Taboola's dossier on Plaintiff De La Torre reveals that he has been classified under multiple segments targeting individuals experiencing financial distress.

These include a first-party Taboola segment classifying him under "Credit card interest users"; an Experian segment identifying him as a "Credit Seeking Card Switcher" with a "High Credit Card Balance"; a segment from Kantar TGI, a consumer research firm that models individuals' financial behaviors from survey data, identifying him as making only minimum payments on credit card debt; and a net asset value segment placing him in the $0–$24,999 range.

118. Perhaps most strikingly, the file contains multiple separate segments sourced from TaxRise, a company that markets tax debt relief services to individuals in financial distress, including segments identifying Plaintiff De La Torre as a person with active tax debt and as an "Active Tax Debt Manager." These segments indicate that TaxRise shared its customer or prospect data with data brokers, who in turn synchronized it with Taboola's system and made them that customer or prospect data available for targeting. As a result, Plaintiff De La Torre's inferred financial condition—his classifications describing difficulty paying off debt and, specifically, his exposure to tax collection—has been packaged into a targeting profile and broadcast to advertisers in real time as he browsed the web.

119. Political Beliefs. Taboola's records reveal an extensive map of Plaintiff De La Torre's political opinions, sourced from i360, a political data firm that constructs detailed voter and ideology profiles on American consumers. The segments assigned to Plaintiff De La Torre include inferred views on specific contested political issues—including his predicted positions on the Second Amendment, immigration, and healthcare policy—as well as classifications of Plaintiff De La Torre as a political donor, a primary voter, and a Democrat-leaning swing voter. In total, Plaintiff De La Torre's profile contains dozens of i360 political classifications, spanning his inferred positions on immigration, healthcare, gun policy, criminal justice, energy, labor, school choice, and reproductive rights.

120. The data file further confirms that many segments were sourced using data from commercial partners including Experian, Kantar, Equifax, Neustar, LiveRamp, and Havas, among others. Each of those relationships represents an additional channel through which Plaintiff De La Torre's personal data has been shared, enriched, and re-broadcast.

121. Plaintiff De La Torre's receipt of the Taboola ID and the thousands of segments contained in the data turned over to him by Taboola confirm that he visited one or more websites in Taboola's publisher network, where Taboola's tracking code executed within his browser. The presence of the segments, including Taboola's first-party segments, in Taboola's dossier on Plaintiff De La Torre indicates that his communications with websites within Taboola's partner network were intercepted by Taboola. As Plaintiff De La Torre browsed the internet, including sites like TurboTax.Intuit.com and HindustanTimes.com, Taboola collected unique personal identifiers and synchronized his identity across its data partners, including Baidu, Tencent, and Temu. Plaintiff De La Torre did not consent to the collection or synchronization of his personal identifiers, nor did he consent to the collection, enrichment, and distribution of detailed information about his online behavior, and was unaware such actions had occurred.

## FACTS SPECIFIC TO PLAINTIFF BAKER

122. Plaintiff John Baker is a resident of Illinois who routinely uses the internet to conduct ordinary activities of daily life, including reading news, managing personal affairs, and researching topics of personal concern. Like the vast majority of Taboola's surveillance targets, Plaintiff Baker had never previously heard of Taboola, has never created an account with Taboola, and has never consented to Taboola's collection, profiling, or dissemination of his personal information.

123. In June 2025, while in Illinois, Plaintiff Baker visited the website abc7chicago.com, a local news website. Unknown to Plaintiff Baker, Taboola's code is deployed on the site and has been designed by Taboola to collect and share the personal information and browsing data of the website's users with numerous parties and to intercept users' communications with the website. Plaintiff Baker was one such user. His information was intercepted, combined with other data, and shared without his permission.

124. While Plaintiff Baker was actively viewing pages on abc7chicago.com, his browser loaded Taboola's JavaScript code, which was embedded on the site. This code executed silently and automatically during the page-load process, without any additional action by Plaintiff Baker. Taboola's code triggered an identity sync to de-anonymize Plaintiff Baker's data across multiple identity providers, including Baidu, Temu, and Tencent, enhancing the ability of Taboola and other third parties to recognize and track Plaintiff Baker across the internet on an ongoing basis. At the same time, Taboola's code initiated automated bid requests sent from Plaintiff Baker's browser to Taboola's servers as part of the real-time bidding auction that monetized his profile.

125. On information and belief, these Taboola-initiated bid requests featured persistent identifiers uniquely associated with Plaintiff Baker, including his cookie IDs, device IDs, IP address, and browser metadata, along with the full URL of the specific page that Plaintiff Baker was viewing at the time. Taboola then enriched these bid requests with other data before sending the data to purchasers of ad inventory. Bid requests of this form routinely include behavioral segment data, which further indicated and revealed Plaintiff Baker's interests and personal characteristics, far beyond what is revealed by the URL itself.

126. On information and belief, these segments, together with page-level context, were broadcast to dozens of advertising technology companies participating in the real-time bidding auction. As a result, these companies received detailed information about Plaintiff Baker's online behavior and interests in real time, without his knowledge or consent.

127. In addition, Taboola initiated user-synchronization with Chinese technology companies linked to the CCP, which transmitted Plaintiff Baker's persistent identifiers—including IP address, advertising identifiers, and cookie data—to Baidu, Tencent, and Temu's servers.

128. Taboola also performed user-synchronization with Plaintiff Baker's information on numerous other websites, including but not limited to syncs with Temu, Tencent, and Baidu on websites like Slate.com and usatoday.com.

129. In July 2026, Plaintiff Baker submitted a data subject access request to Taboola to determine what information Taboola had collected and maintained about him. In response, Taboola disclosed a file revealing that it had assigned Plaintiff Baker a persistent tracking identifier—the Taboola ID (t_gid)—and had used that identifier to accumulate, assign, and make available to third parties hundreds of audience segment classifications describing his personal characteristics, health status, reproductive status, financial condition, and political and demographic profile. Taboola maintains and shares these classifications with countless third parties, regardless of their veracity.

130. The dossier on Plaintiff Baker disclosed by Taboola demonstrates that Taboola has made Plaintiff Baker available for targeting under at least the following sensitive categories:

131. Health. Taboola's records reveal that Plaintiff Baker has been assigned multiple segments describing inferred characteristics concerning health status and behavior. These

segments include a first-party Taboola segment placing Plaintiff Baker in the category "Custom > CTCP > Smokers"; a further Taboola segment, "Contextual > Taboola Medicare Users," associates him with Medicare enrollment, implicating both his age and health-insurance status; and another first-party Taboola segment tied to a named health system, "Custom > Contextual > Novant Health - Cancer custom Segment," displays an inference connecting Plaintiff Baker to cancer-related content. An Eyeota segment separately classifies him within an audience with an interest in "Diet and Weight Loss."

132. Financial Condition. Taboola's data file reveals that Plaintiff Baker has been classified under numerous segments describing his inferred financial condition. These segments include a "Net Asset Value" segment placing Plaintiff Baker in the lowest tier, $0–$24,999; a segment describing Plaintiff Baker's credit level as "Poor"; a Taboola first-party "Credit Monitoring Customers" segment; and a Taboola first-party segment, "Credit Card Debt – Domain Targeting," associating him with consumer credit card debt.

133. Taboola also collects a wealth of other financial inferences about Plaintiff Baker, such as predictions regarding his total invested assets and his likelihood of refinancing his mortgage.

134. Taboola's data also reveals that it has tracked the specific types of credit cards believed to be held by Plaintiff Baker (e.g., "Credit Card Type Have-Amex Platinum") and how recently they appear to have been used. Plaintiff Baker's inferred financial condition has been packaged into a targeting profile and made available to advertisers as he browsed the web.

135. Political Beliefs and Protected Characteristics. Taboola's records reveal an attempt to map Plaintiff Baker's inferred political positions and personal ideology.

136. The file further reflects inferences about Plaintiff Baker's religious life, with one segment identifying him as a "Charitable Donor > Religious," an inferred classification implicating Plaintiff Baker's presumed faith and religious practice. Plaintiff Baker is further classified as a donor to a particular political party, and the file further contains inferences touching other protected characteristics, including a segment classifying Plaintiff Baker within an audience coded "Black" and a segment labeled "LGBT Donors and Supporters." These are not generalized demographic inferences but individualized predictions about Plaintiff Baker's identity and his positions on serious political questions.

137. Personal Life, Relationship Status, and Household Composition. Taboola and its partners have also modeled Plaintiff Baker's relationship status, household composition, and details about his personal life. For example, Taboola's dossier contains segments describing Plaintiff Baker as "Newly Single," "Divorced," and associates him with "Online Dating" activity, together mapping a detailed, inferred narrative of a specific life transition.

138. Taboola's data also details the believed composition of Plaintiff Baker's household, such as segments reflecting the inference that there are "2 Children 6-17" residing in his household, and that a child in his household is female.

139. Additional segments reflect an inferred household income range of "$50,000-59,999," an inferred homeowner's insurance value of "$50,000-$74,999," and a classification that a household member's language preference is English. Each of these labels alone constitutes an invasive inference, but when taken together, the detail of Taboola's inferred map of Plaintiff Baker's personal life is stunning.

140. The data file further confirms that many segments were sourced using data from commercial partners including Experian, Equifax, Neustar, LiveRamp, Eyeota, and Lotame,

among others. Each of those relationships represents an additional channel through which Plaintiff Baker's personal data has been shared, enriched, and re-broadcast.

141. Plaintiff Baker's receipt of the Taboola ID and the more than 1,750 segments contained in the data turned over to him by Taboola confirm that he visited one or more websites in Taboola's publisher network, such as those listed above, where Taboola's tracking code executed within his browser, intercepting the contents of his communications with the website and transmitting his data to Taboola's servers.

142. Based on the allegations herein regarding Taboola's RTB operations and its active identity synchronization integrations with Temu, Tencent, and Baidu, those page views triggered bid requests that included Plaintiff Baker's Taboola ID, IP address, browsing context, and segment data, and broadcast that information to third-party bidders including, on information and belief, Temu, Tencent, and Baidu. During at least one such visit, Taboola intercepted Plaintiff Baker's communications with the website and subsequently synchronized his identifiers with Temu, Tencent, and Baidu. Plaintiff Baker did not consent to any of these interceptions or transmissions and was unaware they had occurred.

## CLASS ACTION ALLEGATIONS

143. **Class Definitions**: Plaintiffs De La Torre and Baker bring this proposed class action pursuant to Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of themselves and the BSD Class and a California Class of all others similarly situated (together, the "Classes"), defined as follows:

> **BSD Class**: All individuals in the United States using a website or application incorporating Taboola's tracking technology whose personal information was transmitted to Baidu, Tencent, Temu, or other entities based in the People's Republic of China on or after April 8, 2025.

> **California Class**: All individuals located in California whose personal information or information derived therefrom Taboola used to create, maintain, or share a profile made available through Taboola's advertising exchange.

Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and its officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

144. **Numerosity**: The exact number of members in the Classes is unknown and not available to Plaintiffs at this time, but individual joinder is impracticable. Defendant has many thousands of internet users who fall into the definition of the Classes. Members of the Classes can be identified through Defendant's records and by reference to other objective criteria.

145. **Commonality and Predominance**: There are questions of law and fact common to the claims of Plaintiffs and the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

(a) Whether Defendant intentionally violated the privacy rights of Plaintiffs and members of the Classes;

(b) Whether Defendant's identity syncing technology caused the unlawful collection and dissemination of the personal data of Plaintiffs and members of the Classes;

(c) Whether Defendant used tracking technologies to cause users' web browsers to reroute electronic communications or other data—including URLs, metadata, and behavioral activity—to Defendant;

(d) Whether Defendant tracked website visitors and caused details about internet users' visits to websites and other private behavior to be intercepted and paired with other personal information about such persons, and disseminated and shared with third parties, including entities controlled by adversaries of the United States, without their knowledge or consent;

(e) Whether Defendant used a device, as defined under 18 U.S.C. section 2510(5), to intercept the contents of communications from Plaintiffs and the Classes;

(f) Whether Defendant obtained valid consent from Plaintiffs and the Classes to intercept and disclose their electronic communications or personal data to third parties;

(g) Whether Defendant tortiously intercepted or otherwise gathered and used the communications and personal data of Plaintiffs and members of the Classes;

(h) Whether Defendant's interception and disclosure of communications from Plaintiffs and the Classes fall within the ECPA's crime-tort exception to the party-exception provision; and

(i) For the California Class, whether Defendant's conduct violated the California Constitution or intruded upon the privacy rights of California residents.

146. **Typicality**: Plaintiffs' claims are typical of the claims of members of the Classes. The claims arise from a common nucleus of operative fact—inter alia, the surreptitious interception and illicit collection and sharing of their personal information. Plaintiffs, like all members of the Classes, had their information unlawfully collected and shared and have been injured by Defendant's misconduct at issue.

147. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the Classes and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs' claims are representative of the claims of the other members of the Classes. That is, Plaintiffs and the members of the Classes sustained injuries and damages as a result of Defendant's conduct. Plaintiffs also have no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have any conflicts with or interests adverse to the Classes.

148. **Superiority**: Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, as joinder of all members of the Classes is impracticable. Individual litigation would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint as well as the risk of inconsistent adjudication. By contrast, a class action presents far fewer management difficulties and provides the benefits of

single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

149. Plaintiffs reserve the right to revise the foregoing "Class Allegations" and "Class Definitions" based on facts learned through additional investigation and in discovery.

**FIRST CAUSE OF ACTION**
**Intrusion Upon Seclusion Under California Common Law**
**(On behalf of Plaintiff De La Torre and the California Class)**

150. Plaintiff De La Torre and the California Class members incorporate the foregoing allegations as if fully set forth herein.

151. Plaintiff De La Torre and the California Class members have a strong interest in preventing the unauthorized collection, aggregation, and dissemination of their most personal information. Plaintiff De La Torre and the California Class also have a strong interest in preventing the compilation and widespread distribution of detailed cradle-to-grave consumer profiles to unknown third parties without their knowledge or consent.

152. These individuals maintain a reasonable expectation of privacy in their day-to-day lives—an expectation that extends not only to their internet browsing activity and online communications, but also to the personal data that Taboola surreptitiously collects, enriches, de-anonymizes, and sells without the knowledge or consent of Plaintiff De La Torre and the California Class members.

153. Taboola intentionally violates Plaintiff De La Torre's and the California Class members' reasonable expectation of privacy through its covert collection, aggregation, correlation, and dissemination of sensitive information and profiles tied to Plaintiff De La Torre and the California Class members as alleged herein.

154. Taboola's business model depends upon the development and offering for sale of increasingly intimate and identifiable consumer profiles. To this end, Taboola's technologies are designed to collect, analyze, monetize, and share sensitive consumer data for targeted advertising and user profiling. Taboola conducts real-time surveillance of users engaging with deeply personal content, capturing a broad array of sensitive data.

155. Taboola intentionally and extensively violates the reasonable expectation of privacy held by Plaintiff De La Torre and the California Class members through engaging in covert, large-scale data collection designed to uniquely identify and surveil individuals. This extensive aggregation, synthesis, and sale of comprehensive online data would be highly offensive to a reasonable person and constitutes an egregious breach of social norms.

156. Taboola covertly harvests and correlates personal information, enriches that data with additional details, and builds highly detailed consumer profiles unique to each individual. Taboola leverages direct data collection, AI analysis and profiling, and its partnerships with third-party data providers to create intimate, identifiable profiles on the individuals it covertly tracks.

157. These enriched profiles are then shared for profit with potentially thousands of undisclosed third parties through the RTB process. These unknown third parties are then empowered to target individuals based on sensitive behavior and inferred characteristics. These cradle-to-grave consumer profiles become more personalized and therefore more valuable the longer they are shared and updated. As these profiles become increasingly personalized, the more trivial it becomes to infer or re-attach a real-world identity to them.

158. Collecting detailed information about a person's device, behavior, or website usage while they engage with personal content is inherently intrusive. Most people would be

shocked to learn that simply opening a webpage could trigger real-time data harvesting and the silent creation of a detailed behavioral profile tied to their identity. This covert surveillance and subsequent profiling would be highly offensive to a reasonable person and constitutes a profound violation of social norms.

159. Taboola does not collect isolated data points from Plaintiff De La Torre and California Class members. Rather, it stockpiles a vast range of personal information, including persistent identifiers (e.g., cookie IDs, device IDs, mobile advertising IDs, and IP addresses), device metadata (e.g., screen resolution, browser version, operating system, and language settings), and contextual information such as full URLs and query parameters. This contextual data often reveals the exact content being viewed on the page (such as the page position the user's browser is scrolled to) by the individual at the very moment Taboola broadcasts the data to bidders.

160. Through these practices, Taboola intercepts, tracks, collects, aggregates, and redistributes the internet activity and communications of Plaintiff De La Torre and California Class members. Taboola's identity-syncing processes link user identifiers across websites and devices, facilitating persistent cross-site tracking and user recognition. This allows Taboola, and those third parties with which Taboola syncs identifiers, to link activity across websites and sessions and compile a detailed, persistent profile that follows individuals across the internet.

161. By combining its role in the RTB ecosystem with technologies like JavaScript trackers and identity-syncing endpoints, Taboola compiles and constantly refines a vast repository of personal data, including the attributes, internet activity, and communications of Plaintiff De La Torre and California Class members.

162. This widespread surveillance and distribution of personal data occur without meaningful disclosure and defies users' reasonable expectations of privacy. No reasonable user would expect that a company like Taboola would track, compile, and sell sensitive information about their health concerns and other private information to a vast network of unknown companies.

163. Taboola does more than record user activity across the internet. Taboola exploits and analyzes vast troves of data to generate inferences about the consumer, including likely interests, health-related concerns, financial condition, and other personal characteristics. Taboola feeds the information it harvests into a massive AI-driven profiling engine trained on the behavioral histories of hundreds of millions of people, designed to predict each individual's interests, vulnerabilities, and likely responses to targeted messaging with ever-increasing precision.

164. A reasonable person who learned that their private health searches, late-night reading habits, financial anxieties, and personal interests had been silently harvested and ingested into a machine built to model and exploit human behavior would not simply feel inconvenienced; they would feel violated. That reaction reflects a reasonable response to the kind of highly offensive intrusion to which Taboola is subjecting millions of people every single day. The covert feeding of intimate human behavior into an industrial-scale AI profiling system without notice, without consent, and without any meaningful ability to stop it is not a routine feature of modern commerce.

165. Taboola's behavioral analysis enables it to create or assign segments to users, classifications that allow Taboola and its downstream partners to categorize each user in a highly personalized manner. These detailed segments are not based only on demographic information

but may also be based on deeply sensitive attributes like mental or physical health conditions, financial distress, political views, disability, and religious beliefs. In addition to segments derived from its own data, it also assigns segments to users based on many data partnerships, essentially commoditizing the act of profiling and tracking users across the web.

166. These segments are shared alongside unique identifying information, providing not just a detailed snapshot of the user's traits but the ability to permanently tie those traits to an infinitely expandable and re-shareable profile on that individual. Taboola shares these highly personalized profiles, including detailed segment data, with potentially thousands of unknown third parties. The information is distributed in real time and may also be retained by these downstream partners, creating additional copies of these profiles that can be used, enhanced, and re-shared indefinitely. By facilitating this process, Taboola not only violates Plaintiff De La Torre's and California Class members' reasonable expectation of privacy but also empowers downstream entities to do the same.

167. Taboola leverages its position in the RTB ecosystem to gain covert and unwanted access to the data of Plaintiff De La Torre and members of the California Class. Compiling that information into detailed consumer profiles that serve as long-term records of an individual's behavior over time, then enabling advertisers and data brokers to tie those profiles to real-world identities, is highly offensive. Sharing those cradle-to-grave consumer profiles containing behavioral and potentially identifying data with a global network of bidders for profit, on an ongoing basis, is highly offensive. Covertly feeding detailed data on intimate human behavior into an industrial-scale AI profiling engine is highly offensive.

168. When a third party participates in an RTB auction through Taboola's platform, it receives behavioral segment data, persistent identifiers, and the context of the web page being

viewed. This allows the third party not only to serve targeted ads but also to retain and analyze that information for future use, thereby gaining expansive, long-term visibility into users' habits, interests, and vulnerabilities.

169. Despite the dangers of sharing this unlawfully gathered data, Taboola knowingly shares sensitive information, including Plaintiff De La Torre's and California Class members' browsing activity, behavioral insights, and personal identifiers, with countless third parties.

170. The extent of Taboola's collection, enrichment, and redistribution of highly detailed consumer profiles is staggering and highly offensive. Taboola's large-scale development and disclosure of extensive consumer profiles for commercial gain represents an egregious breach of social norms and violates the reasonable expectation of privacy held by Plaintiff De La Torre and the California Class members. Taboola lacks any legitimate business interest in covertly tracking, profiling, and aggregating the identities and private information of Plaintiff De La Torre and the California Class members.

171. As a result of these extensive and intentional invasions of privacy, Plaintiff De La Torre and the California Class members have suffered harm and are entitled to just compensation and injunctive relief.

## SECOND CAUSE OF ACTION
### Invasion of Privacy Under the California Constitution
### (On behalf of Plaintiff De La Torre and the California Class)

172. Plaintiff De La Torre and the California Class members incorporate the foregoing allegations as if fully set forth herein.

173. Article I, section one of the California Constitution guarantees to every California citizen the inalienable right to privacy.

174. Plaintiff De La Torre realleges and incorporates by reference the factual allegations set forth in ¶¶ 150-171, which describe Taboola's intentional, highly offensive

invasion of Plaintiff De La Torre's reasonable expectation of privacy, and which independently satisfy the elements of a claim under Article I of the California Constitution.

175. As a result of Taboola's intentional violations of Plaintiff De La Torre's and the California Class members' constitutional right to privacy under the California Constitution, Plaintiff De La Torre and the California Class members have suffered legally cognizable harm and are entitled to just compensation and injunctive relief.

**THIRD CAUSE OF ACTION**
**Violation of the California Invasion of Privacy Act ("CIPA")**
**Cal. Penal Code § 631(a)**
**(On behalf of Plaintiff De La Torre and the California Class)**

176. Plaintiff De La Torre and the California Class members incorporate the foregoing allegations as if fully set forth herein.

177. Plaintiff De La Torre brings this claim on behalf of himself and the California Class under the California Invasion of Privacy Act ("CIPA"), codified in California Penal Code sections 630–38.

178. California Penal Code section 631(a) prohibits, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . 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 who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who 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 above in this section[.]

179. Defendant Taboola knowingly and willfully distributes and maintains and uses tracking scripts, pixels, and other tracking infrastructure on third-party websites for the purpose of duplicating and diverting user communications to Taboola's own servers and those of third parties. Taboola's technologies intentionally capture the contents of users' interactions with these websites and purposefully transmit them to Taboola and its many integrated demand-side partners.

180. Taboola's technologies, including tracking scripts and pixels, constitute "machine[s], instrument[s], or contrivance[s]" under CIPA, and even if they do not, Taboola's deliberate and willful operation of these technologies to facilitate its interceptions falls under CIPA's statutory catch-all category of "any other manner" of tapping or making an unauthorized connection.

181. Taboola's tracking code—JavaScript embedded in the source code of partner websites—executed automatically within Plaintiff De La Torre's and California Class members' browsers during the page load process, contemporaneously with their communications with the website. This code intercepted the contents of Plaintiff De La Torre's and California Class members' interactions with those websites by duplicating and redirecting first-party communications, including full URLs, page titles, and a taxonomical classification of the content of the page, to Taboola and other third parties. These interceptions occurred as part of the browser's rendering sequence, in parallel with the requests to the host website, before Plaintiff De La Torre or members of the California Class could detect, review, or prevent the transmissions.

182. As users like Plaintiff De La Torre and the California Class members navigate websites such as TurboTax.Intuit.com, Taboola's JavaScript code causes their browsers to transmit full URLs, page titles, and other page-level metadata to Taboola's servers in real time. These transmissions occur without the user's awareness or consent and are initiated automatically during the same browser session in which the user communicates with the website.

183. The data intercepted by Taboola from Plaintiff De La Torre and California Class members includes full-page URLs. Taboola reads and redistributes the URL and related contextual information as part of the RTB auction process, learning the contents and context of these communications by Plaintiff De La Torre and California Class members before the webpage has even finished loading.

184. Taboola's unlawful interception of communications occurred in a manner that was not authorized by Plaintiff De La Torre or California Class Members, who did not consent to Taboola's tracking, compilation, or use of their identity and communications content across the internet.

185. Plaintiff De La Torre and members of the California Class suffered harm as a result of Defendant's violations of the California Invasion of Privacy Act and seek injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to California Penal Code section 637.2(a).

## FOURTH CAUSE OF ACTION
**Violation of Electronic Communications Privacy Act ("ECPA")**
**18 U.S.C. § 2510, et seq.**
**(On behalf of Plaintiffs De La Torre and Baker and the Classes)**

186. Plaintiffs De La Torre and Baker and members of the Classes incorporate the foregoing allegations as if fully set forth herein.

187. The ECPA prohibits any person from "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

188. **Intentional Interception**: Defendant Taboola intentionally distributes, maintains, and uses tracking scripts, pixels, and other tracking infrastructure on third-party websites that reroute user communications to Taboola's own servers and those of third parties. Taboola's technologies intentionally capture the contents of users' interactions with these websites and purposefully transmit them to Taboola and its integrated demand-side partners, including foreign buyers. Taboola's tracking code—JavaScript embedded in the source code of partner websites—executed automatically within Plaintiffs' and members of the Classes' browsers during the page load process. This code intercepted the contents of Plaintiffs' and members of the Classes' interactions with those websites by rerouting first-party communications—including full URLs, page titles, and a taxonomical classification of the content of the page—to Taboola and other third parties. These interceptions occurred as part of the browser's rendering sequence, before Plaintiffs or members of the Classes could detect, review, or prevent the transmissions.

189. As users like Plaintiffs and members of the Classes navigate websites such as Slate.com and TurboTax.Intuit.com, Taboola's JavaScript code causes their browsers to transmit full URLs, page titles, and other page-level metadata to Taboola's servers in real time. These transmissions occur without the user's awareness or consent and are initiated automatically during the same browser session in which the user communicates with the website. Taboola's capture of these communications constitutes an unlawful interception under the ECPA.

190. **Contents of a Communication**: The data intercepted by Taboola from Plaintiffs and members of the Classes includes full-page URLs. These qualify as the "contents" of a

communication under 18 U.S.C. § 2510(8) because they reveal the substance and subject matter of the user's communications with the host website.

191. **Use of a Device**: The technologies Taboola uses to intercept this data—including JavaScript and tracking pixels—constitute "devices" under 18 U.S.C. § 2510(5), which includes any device or apparatus used to intercept electronic communications.

192. **Lack of Consent**: Plaintiffs and members of the Classes did not consent to Taboola's interception or disclosure of their communications. Taboola did not provide clear or conspicuous notice that user interactions with publisher websites would be surveilled and routed to foreign entities, and Plaintiffs and members of the Classes lack a reasonable means to detect, prevent, or opt out of Taboola's data collection and sharing. There was no actual or implied consent under applicable law, as no reasonable person would agree to having secret cradle-to-grave consumer profiles built about them, or to have their personal information diverted to a foreign adversary.

193. **Application of the Crime-Tort Exception on Behalf of Plaintiff Baker and the BSD Class**: Even if Taboola were deemed a party to these communications, which it is not, the "party exception" in 18 U.S.C. § 2511(2)(d) does not apply. At the time of the interception, Taboola's interception and use of these communications was undertaken knowingly and intentionally for the independent purpose of committing criminal and tortious acts: with respect to Plaintiff Baker and the BSD Class, the unlawful transmission of bulk U.S. sensitive personal data to a covered foreign entity in violation of the BSD Rule, 28 C.F.R. Part 202.

194. On or after April 8, 2025, Taboola knowingly engaged in prohibited data-brokerage transactions with Chinese technology companies including Temu, Baidu, and Tencent,

all foreign-owned entities with their principal places of business in China, in violation of the BSD Rule. 28 C.F.R. § 202.301(a).

195. Taboola is a corporation organized and existing under the laws of Delaware, with its principal place of business located in the State of New York. Because Taboola, Inc. is organized under the laws of the United States and is an entity in the United States, Taboola is a "U.S. person" under 28 C.F.R. § 202.256.

196. Tencent Holdings Ltd. qualifies as a "covered person" under 28 C.F.R. § 202.211(a) because it is a Chinese company, headquartered in Shenzhen, China, with substantial operations and executive oversight in the People's Republic of China, a "country of concern" under the BSD Rule.

197. Baidu, Inc. qualifies as a "covered person" under 28 C.F.R. § 202.211(a) because it is a Chinese company, headquartered in Beijing, with substantial operations and executive oversight in the People's Republic of China, a "country of concern" under the BSD Rule.

198. Temu qualifies as a "covered person" under 28 C.F.R. § 202.211(a) because it is operated and controlled by PDD Holdings, Inc., a Chinese company with substantial operations and executive oversight in the People's Republic of China, a "country of concern" under the BSD Rule. Although PDD Holdings nominally lists its principal executive offices in Ireland, it maintains a significant presence in China.

199. Like Tencent and Baidu, Temu is subject to Chinese law, including China's National Intelligence Law, Cybersecurity Law, and Data Security Law. These laws compel Chinese companies and individuals to secretly cooperate with government surveillance efforts and grant authorities unrestricted access to private user data. The operations of Tencent, Baidu,

and Temu are therefore presumptively subject to Chinese government control, oversight, and compelled disclosure obligations.

200. On websites such as abc7chicago.com visited by Plaintiff Baker, and the websites visited by members of the BSD Class, Taboola initiates identity synchronization requests with Baidu and Temu's infrastructure—and, on information and belief, Tencent infrastructure—which result in the transmission of numerous protected "listed identifiers" under the BSD Rule, including but not limited to IP addresses (28 C.F.R. § 202.234(g)), advertising IDs (28 C.F.R. § 202.234(e)), and cookie data (28 C.F.R. § 202.234(g)).

201. Taboola transmits these protected identifiers together, including, for example, transmitting a given user's IP address along with the user's cookie data and Taboola's t_gid identifier, such that the identifiers are clearly linked with one another and are associated or reasonably capable of being associated with each related user.

202. While the above already represents a significant violation of user privacy, on information and belief, the full scope of user data that Defendant transmits to Baidu, Temu, and Tencent—enabled through standard identifiers in real-time bidding—goes well beyond what an end user can directly observe. On information and belief, server-to-server communications between Taboola and these Chinese companies transmit information such as device IDs (28 C.F.R. § 202.234(c)), user behavioral signals, and a multitude of other advertising identifiers, all made available to the companies to further refine their consumer profiles and enhance their advertising business.

203. This information qualifies as "covered personal identifiers" and "sensitive personal data" under the BSD Rule because these identifiers are shared with Baidu, Temu, and Tencent (1) in combination with at least one other listed identifier, or (2) in combination with

other data such that the listed identifier is or can reasonably be associated with other listed identifiers or other sensitive personal data. 28 C.F.R. §§ 202.212(a), 202.249(a).

204. On information and belief, Taboola has collected or maintained this sensitive personal data relating to more than 100,000 U.S. persons (including Plaintiff Baker and the BSD Class members) following the effective date of the BSD Rule, and therefore this information constitutes "bulk U.S. sensitive personal data" under 28 C.F.R. § 202.206.

205. On information and belief, Taboola provides this information to Baidu, Temu, and Tencent as part of independent commercial transactions between Taboola and the Chinese companies. Neither Baidu, Temu, nor Tencent itself collected or processed this data directly from the relevant individuals, and Taboola's provision of this bulk U.S. sensitive data to Baidu, Temu, and Tencent, covered persons, constitutes "covered data transaction[s] involving data brokerage" under 28 C.F.R. §§ 202.210, 202.214, and 202.214(b)(4)–(9).

206. Taboola is a sophisticated entity in the digital advertising industry. It is a member of industry associations that directly participated in the BSD Rule rulemaking process and publicly warned members of the legal risks of transmitting certain data to entities based in China. Taboola also acknowledged in its own SEC filings that it actively monitors privacy and data transfer regulations. For these reasons, Taboola knew or reasonably should have known that it had engaged and was engaging in covered data transactions involving data brokerage in violation of the BSD Rule.

207. Because Taboola knowingly engaged and engages in covered data transactions involving data brokerage with Baidu, Temu, and Tencent, each a covered person, Taboola has violated the BSD Rule's prohibition of data-brokerage transactions under 28 C.F.R. § 202.301(a).

208. Because Taboola intentionally and knowingly intercepted and disclosed Plaintiff Baker's and the BSD Class members' communications for the purpose of committing these criminal and tortious acts, it is not shielded by the "party exception" under the ECPA.

209. **Application of the Crime-Tort Exception on Behalf of Plaintiff De La Torre and the California Class**: At the time of the interception, Taboola's interception of the at-issue communications was knowingly and intentionally performed for the independent purpose of committing tortious acts in violation of California law, specifically:

a. Committing the tort of intrusion upon seclusion under California common law by using the contents of the intercepted communications to facilitate the creation of highly detailed consumer profiles on Plaintiff De La Torre and California Class members, which were then used and disseminated as described herein;

b. Committing the tort of intrusion upon seclusion under California common law by covertly syncing Plaintiff De La Torre's and California Class members' unique identifiers with third parties, including entities affiliated with adversarial foreign governments and their militaries, thereby enabling pervasive tracking of Plaintiff De La Torre and California Class members across the internet as described herein;

c. Violating the right to privacy conferred by the California Constitution through the creation and dissemination of highly detailed consumer profiles, enriched by the contents of Plaintiff De La Torre's and the California Class members' communications intercepted by Taboola, as described herein; and

d. Violating the right to privacy conferred by the California Constitution by covertly syncing Plaintiff De La Torre's and California Class members' unique identifiers with third parties, including entities affiliated with adversarial foreign governments and their

militaries, thereby enabling pervasive tracking of Plaintiff De La Torre and California Class members across the internet as described herein.

210. Because Taboola intentionally and knowingly intercepted and disclosed Plaintiff De La Torre's and California Class members' communications for the purpose of committing these tortious acts, it is not shielded by the "party exception" under the ECPA.

211. Plaintiffs De La Torre and Baker and the Classes have suffered and continue to suffer harm as a result of Defendant's violations of the ECPA, including the transmission of Plaintiff Baker's and BSD Class members' sensitive data to a foreign adversary, and the creation of cradle-to-grave consumer profiles on Plaintiffs De La Torre and Baker and members of the Classes, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and disgorgement of profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(c)(2), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs De La Torre and Baker, individually and on behalf of the Classes, pray for the following relief:

(a) An order certifying the California Class and BSD Class as defined above, appointing Plaintiff De La Torre as the representative of the California Class and Plaintiff Baker as the representative of the BSD Class, and appointing their counsel as Class Counsel;

(b) A judgment holding that Defendant's actions, as set out above, violate the ECPA, 18 U.S.C. § 2510, et seq., with respect to Plaintiffs De La Torre and Baker and the Classes, and

that Defendant's actions violate the California Constitution and intrude upon the seclusion of Plaintiff De La Torre and members of the California Class;

(c) A judgment holding that Defendant's actions, as set out above, violate CIPA, Cal. Penal Code § 631(a), with respect to Plaintiff De La Torre and the California Class;

(d) An injunction requiring Defendant to cease all unlawful activities;

(e) A judgment awarding statutory damages, disgorgement of profits, punitive damages, costs, and attorneys' fees; and

(f) Such other and further relief that the Court deems reasonable and just.

**JURY DEMAND**

Plaintiffs request a trial by jury of all claims that can be so tried.

Respectfully submitted,

**ALESSANDRO DE LA TORRE** and **JOHN BAKER**, individually and on behalf of all others similarly situated,

Dated: July 24, 2026

By: */s/ Michael W. Ovca*

Michael W. Ovca (*pro hac vice* forthcoming)
movca@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

*Counsel for Plaintiffs and the Putative Classes*