Todd M. Friedman, Esq. (SBN 216752)
Adrian R. Bacon, Esq. (SBN 280332)
LAW OFFICES OF TODD M. FRIEDMAN, P.C.
21301 Ventura Blvd, Suite 340
Woodland Hills, CA 91364
Phone: (323) 306-4234
Fax: (866) 633-0228
tfriedman@toddflaw.com
abacon@toddflaw.com
Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES
UNLIMITED JURISDICTION

REBEKA RODRIGUEZ, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FANDUEL INC., a Delaware corporation d/b/a WWW.FANDUEL.COM,

Defendant.

Case No. 24STCV30655

CLASS ACTION COMPLAINT FOR VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT

(Amount to Exceed $35,000)

INTRODUCTION

1. Californians increasingly conduct their lives and activities over the Internet, sharing often sensitive personal information with companies by using company websites rather than landline telephones.

2. Defendant created its own online presence at ***fanduel.com*** (the "Website") to communicate with potential customers, encouraging engagement with this electronic medium – Defendant's Website -- as an alternative to the telephonic or in-person interaction. Defendant did this to enable potential customers to obtain information from and about Defendant's goods and services, and to enable Defendant to elicit information from potential customers about their specific needs and desires.

3. Defendant well understands that its Website is a means to communicate privately with potential customers – a consumer expectation that is not only reasonable, but actively nurtured by Defendant. Indeed, Defendant assures visitors to its website that ***"Fanduel recognizes that people who use FanDuel's Service value their privacy."*** *See* www.fanduel.com/privacy (last accessed November 2024).

4. Defendant's promise is false. In reality, Defendant aids a third party (ByteDance, a Beijing-based company that owns and controls TikTok and which is under investigation by the United States Department of Justice for spying on American citizens) to surveil its interactions with visitors to its Website, thereby allowing TikTok to create detailed portraits of Website visitors' interests, needs, and desires.[1]

5. In short, Defendant falsely promised Website visitors that it would protect their privacy, but then secretly monetized their personal information by enabling TikTok to spy on those visitors, surveil their journey across the web, track their location and lifestyle habits, and bombard them with targeted advertising. Rather than candidly disclose this arrangement, Defendant explicitly and implicitly assured Website visitors that their identities and privacy would be protected. In short, Defendant lied.

[1] While the allegations in this Complaint focus on ByteDance and TikTok, the website plays host to a cornucopia of other invasive tracking and surveillance products, details of which will be explored in discovery.

6. In words too plain to question, the California Legislature has made clear that the secret TikTok surveillance that occurred here falls squarely within CIPA's protective ambit. Those same words show that the Legislature intended that such secret surveillance would not escape CIPA's reach, even when it occurs over a website on the Internet rather than over a telephone or telegraph.

7. Plaintiff visited Defendant's Website in the latter part of 2024. As summarized above and shown below, Defendant secretly deployed a de-anonymization process to identify and track Plaintiff using electronic impulses generated from Plaintiff's device. Defendant's actions violate California's Trap and Trace Law, codified at California Penal Code § 638.51.

JURISDICTION AND VENUE

8. As a Court of general jurisdiction, This Court has jurisdiction over all matters presented to it per the mandates of the California Constitution.

9. Venue is proper in this County because some of the class members' claims arose in this county.

10. Defendant is subject to jurisdiction under California's "long-arm" statute found at California Code of Civil Procedure Section 410.10 because the exercise of jurisdiction over Defendant is not "inconsistent with the Constitution of this state or the United States." Indeed, Plaintiff believes that Defendant generates a minimum of eight percent of its national sales to Californians, such that the website "is the equivalent of a physical store in California." Since this case involves illegal conduct emanating from Defendant's operation of its Website targeting Californians, California courts can "properly exercise personal jurisdiction" over the Defendant in accordance with the Court of Appeal opinion in *Thurston v. Fairfield Collectibles of Georgia*, 53 Cal. App. 5th 1231, 1235 (2020).

PARTIES

11. Plaintiff is a resident and citizen of California.

12. Defendant is New York entity that operates online gambling activities.

FACTUAL ALLEGATIONS

Defendant's Website and the Tik Tok Software Spies on Activists Like Plaintiff.

13. Defendant operates the Website. Defendant has installed on its Website software created by TikTok in order to identify website visitors (the "TikTok Software").

14. The TikTok Software acts via a process known as "fingerprinting." Put simply, the TikTok Software collects as much data as it can about an otherwise anonymous visitor to the Website and matches it with existing data TikTok has acquired and accumulated about hundreds of millions of Americans.

15. The TikTok Software gathers device and browser information, geographic information, referral tracking, and url tracking by running code or "scripts" on the Website to send user details to TikTok.

16. The TikTok Software begins to collect information the moment a user lands on the Website before any pop-up or cookie banner advises users of the invasion or seeks their consent.

17. The TikTok Software also requests, validates, and transmits other identifying information, including a website visitor's phone numbers and email addresses.

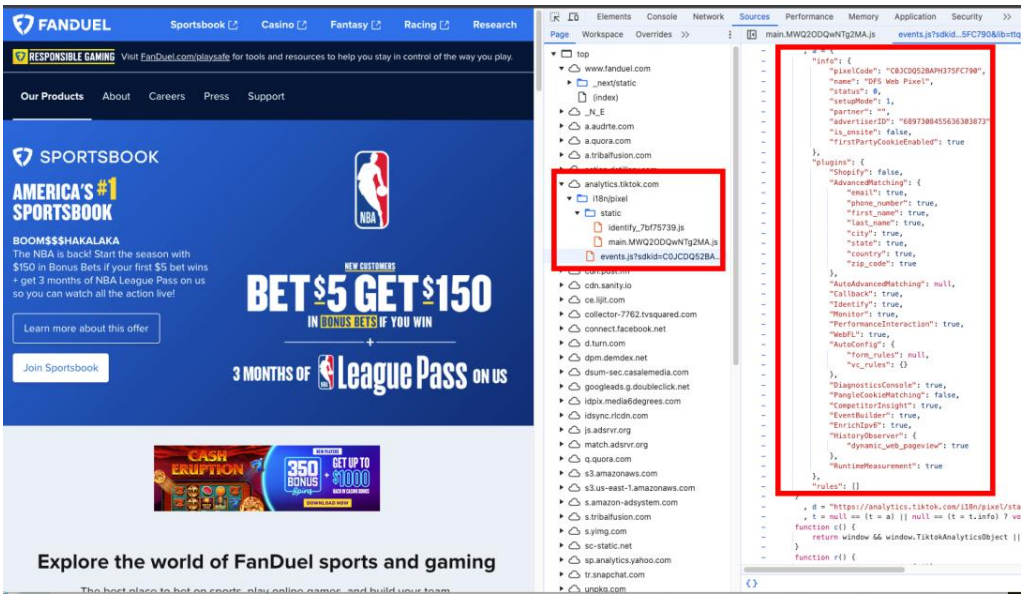
18. According to a leading data security firm, the TikTok tracking pixel secretly installed on Defendant's website is particularly invasive. The pixel "immediately links to data harvesting platforms that pick off usernames and passwords, credit card and banking information and details about users' personal health." The pixel also collects "names, passwords and authentication codes" and "transfer the data to locations around the globe, including China and Russia", and does so "before users have a chance to accept cookies or otherwise grant consent." *See Aaron Katersky*, **TikTok Has Your Data Even If You've Never Used The App: Report**, ABC News (last accessed October 2024), https://abcnews.go.com/Business/tiktok-data-app-report/story?id=97913249.

19. By sharing plaintiff's and class members' personal and de-anonymized data with TikTok, Defendant effectively "doxed" them to America's most formidable geopolitical adversary. *See* https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html, ***Analysis: There is now some public evidence that China viewed TikTok data*** (quoting sworn testimony from former employee But Yu that Chinese Communist Party officials "used a so-called 'god credential' to bypass any privacy protections to spy on civil rights activists' 'unique user data, locations, and communications.'") (last accessed October 2024).

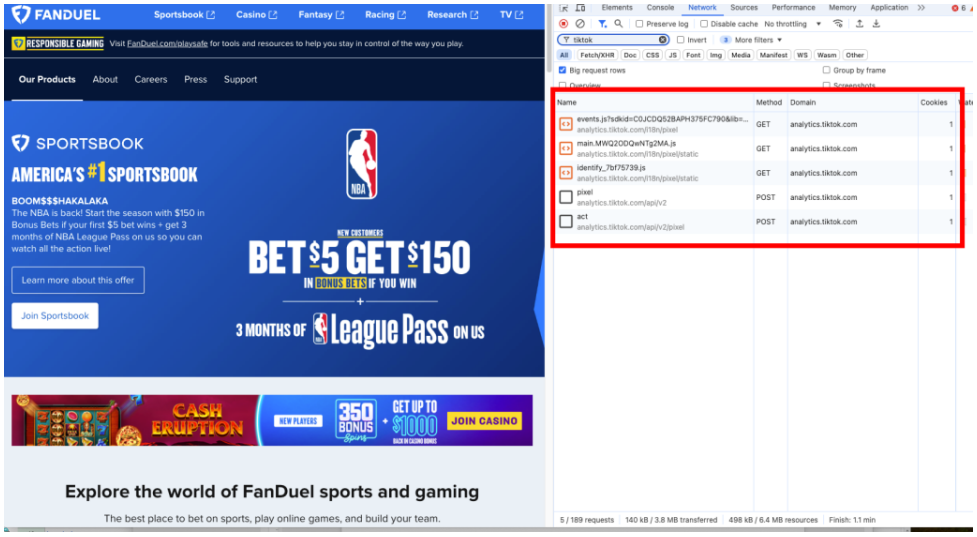
20. Plaintiff is both (1) genuinely interested in the goods, services, and information available on Defendant's Website, and (2) a consumer privacy advocate who works as a "tester" to ensure that

companies abide by the privacy obligations imposed by California law. As the Ninth Circuit recently made exceptionally clear that it is "necessary and desirable for committed individuals to bring serial litigation" to enforce and advance consumer protection statutes, and that Courts must not make any impermissible credibility or standing inferences against them. *Langer v. Kiser*, 57 F.4th 1085, 1095 (9th Cir. 2023). In other words, Plaintiff is exactly the type of person who the Chinese Communist Party has used TikTok to spy upon in the past.

21. An image of the invasive TikTok code secretly embedded on Defendant's Website and which is automatically deployed on the browser, without consent provided by the user, can be see can here:



22. The Website instantly sends communications to TikTok when a user views the page and tracks page interactions. In the example below, the right side of the image shows the various TikTok scripts being run by Defendant, and the electronic impulses being sent to TikTok to add to their collection of user behavior:



The TikTok Software is a Trap and Trace Device.

23. California law defines a "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." California Penal Code § 638.50(c).

24. The TikTok Software is a process to identify the source of electronic communication by capturing incoming electronic impulses and identifying dialing, routing, addressing, and signaling information generated by users, who are never informed that the website is collaborating with the Chinese government to obtain their phone number and other identifying information.

25. The TikTok Software is "reasonably likely" to identify the source of incoming electronic impulses. In fact, it is designed solely to meet this objective.

26. Defendant did not obtain Plaintiff's express or implied consent to be subjected to data sharing with TikTok for the purposes of fingerprinting and de-anonymization.

27. CIPA imposes civil liability and statutory penalties for the installation of trap and trace software without a court order. California Penal Code § 637.2; *see also Greenley v. Kochava*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023). No court order to install a trap and trace device via the TikTok Software was obtained by Defendant.

28. Defendant did not obtain Plaintiff's or class members' express or implied consent to be subjected to data sharing with TikTok for the purposes of fingerprinting and de-anonymization.

CLASS ALLEGATIONS

29. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class") defined as follows:

> **All California citizens whose personal information was shared with TikTok or other third parties by Defendant without their effective and informed prior consent.**

30. NUMEROSITY: Plaintiff does not know the number of Class Members but believes the number to be in the tens of thousands. The exact identities of Class Members may be ascertained by the records maintained by Defendant.

31. COMMONALITY: Common questions of fact and law exist as to all Class Members, and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class Member, include but are not limited to the following:

a. Whether Defendant shared class members' personal information with TikTok or other third parties;

b. Whether Defendant obtain effective and informed consent to do so;

c. Whether Plaintiff and Class Members are entitled to statutory penalties; and

d. Whether Class Members are entitled to injunctive relief.

32. TYPICALITY: As a person who visited Defendant's Website and whose personal information was shared by Defendant, Plaintiff is asserting claims that are typical of the Class.

33. ADEQUACY: Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained attorneys experienced in the class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the class or whose inclusion would otherwise be improper are excluded.

34. SUPERIORITY: A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class members is impracticable and inefficient. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

CAUSE OF ACTION

CAUSE OF ACTION

Violations of the California Trap and Trace Law

Cal. Penal Code § 638.51

35. Plaintiff incorporates by reference the foregoing paragraphs as if set forth hereinafter.

36. California's Trap and Trace Law is part of the California Invasion of Privacy Act ("CIPA") codified at Cal. Penal Code 630 *et seq*.

37. CIPA was enacted to curb "the invasion of privacy resulting from the continual and increasing use of" certain technologies determined to pose "a serious threat to the free exercise of personal liberties." CIPA extends civil liability for various means of surveillance using technology, including the installation of a trap and trace device.

38. A "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." California Penal Code § 638.50(c).

39. California Penal Code § 638.51 provides that "a person may not install or use…a trap and trace device without first obtaining a court order…" § 638.51(a). No court order to install a trap and trace device via the TikTok Software was obtained by Defendant.

40. Defendant uses a trap and trace process on its Website by deploying the TikTok Software on its Website, because the software is designed to capture the phone number, email, routing, addressing and other signaling information of website visitors. As such, the TikTok Software is solely to identify the source of the incoming electronic and wire communications to the Website.

41. Defendant did not obtain consent from Plaintiff and class members before using trap and trace technology to identify users of its Website, and has violated Section 638.51.

42. CIPA imposes civil liability and statutory penalties for violations of § 638.51.

43. Therefore, Plaintiff and class members are entitled to the relief set forth below.

PRAYER

WHEREFORE, Plaintiff prays for the following relief against Defendant:

1. An order certifying the class and making all appropriate class management orders;

2. Statutory damages pursuant to CIPA;

3. Reasonable attorneys' fees and costs; and

4. All other relief that would be just and proper as a matter of law or equity, as determined by the Court.

Dated: November 20, 2024

LAW OFFICES OF TODD M. FRIEDMAN, P.C.

By: Todd M. Friedman

Todd M. Friedman, Esq.
Attorneys for Plaintiff