

Victor J. Sandoval (SBN 344461)
ALMEIDA LAW GROUP LLC
3415 S. Sepulveda Blvd. Suite 1121
Los Angeles, California 90034
(562) 534-5907
victor@almeidalawgroup.com

Attorneys for Plaintiff & the Putative Classes

[additional counsel on signature page]

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

M.C. 1 and M.C. 2, by and through their legal
guardian HEIDI SAAS, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

WALLWISHER, INC., d/b/a PADLET,

Defendant.

Civ. No. 3:26-cv-10369

CLASS ACTION COMPLAINT FOR:

- 1. Violation of 18 U.S.C. § 2510 *et seq.***
- 2. Violation of Cal. Penal Code § 631**
- 3. Violation of Cal. Penal Code § 632**
- 4. Violation of Cal. Penal Code § 502 *et seq.***
- 5. Violation of Cal. Bus. & Prof. Code § 17200 *et seq.***
- 6. Invasion of Privacy – Intrusion Upon Seclusion**
- 7. Violation of Md. Code, Cts. & Jud. Proc. §§ 10-401 *et seq.***
- 8. Unjust Enrichment – Quasi Contract**

JURY TRIAL DEMANDED

1 M.C. 1¹ and M.C. 2, by and through their mother and legal guardian, Heidi Saas
 2 (“Plaintiffs”), individually and on behalf of all other similarly situated individuals, by and through
 3 their attorneys, bring this class action complaint (“Complaint”) for injunctive and monetary relief
 4 under Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) against Defendant Wallwisher, Inc.
 5 d/b/a Padlet (“Padlet”) and make the following allegations based upon knowledge as to themselves
 6 and the acts of themselves, and upon information and belief as to all other matters.

7 I. INTRODUCTION

8 1. This case is about a private technology company that surreptitiously built its
 9 business by collecting, using, and disclosing children’s personal information—without parental
 10 consent—inside America’s public schools. Defendant Padlet markets its platforms as a privacy-
 11 respecting classroom tool for K–12 instruction. In reality, Padlet functions as a data-harvesting
 12 operation that systematically collects and exploits children’s personal information in violation of
 13 the Children’s Online Privacy Protection Act (“COPPA”)² and other laws.

14 2. Across the United States every day, millions of public schoolchildren enter
 15 classrooms to receive the education to which they are legally entitled. Increasingly, however, that
 16 education is delivered not through textbooks and paper assignments, but through web-based
 17 applications accessed on school-issued devices. These applications—marketed as “education
 18 technology” or “EdTech”—are now embedded into the core of K–12 instruction. Padlet is one such
 19 application. Schools that integrate Padlet’s digital product (“Padlet Platform”) directly into
 20 classroom instruction require students to use its online bulletin boards, whiteboards, and
 21 AI-powered tools for assignments and to submit their work, comments, images, and recordings,
 22 leaving students and parents unable to decline its use without jeopardizing their education.

23 3. While K–12 students use the Padlet Platform to perform their classroom tasks,
 24 Padlet secretly captures a sweeping array of detailed personal information from them, including
 25 children under the age of thirteen, in real time. This personal information (“PI”) includes persistent,

26
 27 ¹ Each minor child’s name has been anonymized, and they will be referred to herein as Minor Child
 (“M.C.”).

28 ² 15 U.S.C. §§ 6501, *et seq.*

1 unique identifiers; device and browser data; precise behavioral data; content students create,
2 upload, and share; and detailed records of how students interact with Padlet, much of which
3 identifies or is reasonably capable of being linked to a specific child. COPPA strictly limits such
4 conduct for children under 13. Before collecting or disclosing the personal information of children
5 under 13, operators of online services must provide clear notice to parents and obtain verifiable
6 parental consent. Padlet does neither.

7 4. Rather than complying with COPPA, Padlet attempts to shift responsibility to
8 schools, asserting—explicitly or implicitly—that schools may consent to Padlet’s data practices on
9 families’ behalf. That assertion is wrong as a matter of law. COPPA places the duty to notify parents
10 and obtain verifiable parental consent squarely on the operator of the online service. Schools have
11 no authority to waive children’s statutory privacy rights so that a private company may exploit
12 student data for its own commercial purposes.

13 5. Against this backdrop, Padlet’s conduct is particularly egregious because Padlet
14 falsely claims that it does not share PI with third parties for advertising or direct-marketing
15 purposes. But forensic analysis of the Padlet Platform proves otherwise. This testing revealed that
16 Padlet effectively has no guard rails and shares extensive PI taken from its child users with more
17 than 160 third parties—including Meta and Google—many of which are advertising-technology
18 companies (“AdTech companies”), including data brokers, identity-resolution companies, and
19 customer-data platforms. These AdTech companies have no legitimate educational purpose for
20 receiving or using students’ data, and their business models depend on aggregating, creating
21 profiles with, and monetizing personal data for targeted advertising and other commercial purposes.

22 6. Forensic testing specifically shows that Padlet shares a broad range of PI, including
23 students’ names, email addresses, and user IDs; behavioral data reflecting how students interact
24 with the Padlet Platform such as pages viewed and time spent; device- and browser-level
25 information; and persistent and unique identifiers that are essentially linkage keys allowing children
26 to be recognized repeatedly across sessions and devices. Padlet instantaneously transmits this PI to
27 major AdTech companies that are capable of linking Padlet classroom activity to extensive,
28

1 preexisting commercial profiles and identities maintained outside the educational environment.

2 7. By combining real-time capture of students' classroom activity with persistent
3 unique identifiers that allow tracking of their activity over time and across multiple websites, Padlet
4 converts educational interactions into individualized behavioral monitoring and facilitates the
5 creation and monetization of detailed dossiers about children, without disclosure, parental consent,
6 or any legitimate educational justification.

7 8. Padlet's collection and disclosure of student data are not incidental to its educational
8 offerings; they are central to its business strategy. After extracting the PI, Padlet uses the students'
9 PI to build, improve, and monetize its products and to confer value on the third-party companies
10 with which it shares student data. These practices confer substantial commercial benefits on Padlet
11 while inflicting significant privacy harms on students and families.

12 9. Padlet does not clearly disclose these practices to parents or students. Rather, Padlet
13 makes vague and misleading statements about how PI is used and implies that schools—not
14 Padlet—are responsible for privacy compliance. It also obscures the extent to which students'
15 information is transmitted to AdTech companies for non-educational purposes. These
16 representations are materially deceptive and misleading.

17 10. Privacy is a fundamental right. Children have a right to privacy in the information
18 that is generated and taken from them, including when at school. Parents have a right to determine
19 who may access that information and for what purpose, and the right to determine whether certain
20 information is created in the first place. Padlet's data practices force students and their families to
21 forgo these essential rights in order to receive the education to which they are legally entitled.
22 Parents and students cannot be expected to surrender their longstanding authority to make critical
23 decisions about children's PI simply to participate in foundational schooling, as is their right.

24 11. Through this action, Plaintiffs and Class members (defined *infra*) seek to hold Padlet
25 accountable for its unlawful data practices, restore transparency and choice to families, and ensure
26 that education technology companies cannot profit by quietly commercializing children's personal
27 information without effective consent.
28

II. JURISDICTION AND VENUE

12. This Court has original jurisdiction over the action under the Class Action Fairness Act (“CAFA”) of 2005. Pursuant to 28 U.S.C. §§ 1332(d)(2) and (6), this Court has original jurisdiction because the aggregate claims of the putative Class members exceed \$5 million, exclusive of interests and costs, and at least one member of the proposed Class is a citizen of a different state than Defendant Padlet.

13. This Court also has subject-matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint alleges a question of federal law, specifically the Federal Wiretap Act (18 U.S.C. §§ 2510, *et seq.*) and a state-law claim premised on a question of federal law, specifically COPPA (15 U.S.C. §§ 6501 *et seq.*; 16 C.F.R. § 312).

14. Venue is proper in this District under 28 U.S.C. § 1391 because Padlet is subject to personal jurisdiction here, regularly conducts business in this District (including but not limited to being headquartered in this District), and because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

15. Further, the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated in part from this District. Padlet has sufficient minimum contacts with this state and sufficiently avails itself of the markets of this state through its promotion, sales, licensing, activities, and marketing within this state. Padlet purposely availed itself of the laws of California and engaged and is engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including persons Padlet knew or had reason to know are located in California, including in this District.

16. Further, Padlet’s Terms of Service, dated May 6, 2026, include a forum-selection clause that states, “You agree that any claim or dispute you may have against Padlet must be resolved exclusively by a state or federal court located in the City and County of San Francisco, California, except as otherwise agreed by the parties. You agree to submit to the personal jurisdiction of the courts located within City and County San Francisco, San Francisco for the purpose of litigating all such claims or disputes.” Without conceding—and indeed disputing—that

1 Padlet's Terms of Service are binding on Plaintiffs and any putative class members, Padlet's
 2 inclusion of this provision in its Terms of Service estops Padlet from challenging jurisdiction or
 3 venue for an action brought in this District.

4 17. California law applies to the claims of Plaintiffs and Class members.

5 18. Under California's choice-of-law rules, "[w]hether a nonresident plaintiff can
 6 assert a claim under California law is a constitutional question based on whether California has
 7 sufficiently significant contacts with the plaintiff's claims." *Opperman v. Path, Inc.*, 87 F.Supp.3d
 8 1018, 1040 (N.D. Cal. 2014).

9 19. The claims here meet this "sufficiently significant contacts" test, given Padlet's
 10 myriad contacts with the State of California, which include, *inter alia*, the following:

- 11 a. Padlet is headquartered in California;
- 12 b. At all times relevant to this litigation, Padlet has conducted a significant portion of
- 13 its business in California;
- 14 c. Padlet's decisions to create its platform (including the portions of the platform that
- 15 siphon children's personal information without consent) and to release the
- 16 platform into the stream of commerce emanated from California;
- 17 d. Padlet designed its platform in California;
- 18 e. As of the date of this filing, the majority of U.S.-based Padlet employees,
- 19 including its CEO, work in its San Francisco office, including employees involved
- 20 in the following areas: Design, Product, Engineering, Marketing, Customer Ops,
- 21 Operations, and Sales³; and
- 22 f. As of the date of this filing, all U.S.-based jobs offered at Padlet are in San
- 23 Francisco, California (with the lone exception of a remote position for Account
- 24 Executive). The jobs include, *inter alia*, Head of Design; Senior Product Designer;
- 25
- 26

27 ³ *The Natural Inanity Behind the Artificial Intelligence*, Padlet, <https://padlet.jobs/comrades> (last
 28 visited Aug. 31, 2026).

Software Engineer – Frontend/Backend/Fullstack; Software Engineer – Mobile; Business Development Representative; and Sales Operations Manager.⁴

20. Because of the contacts that Padlet has with California, there are sufficient significant contacts with California to allow non-Californian Plaintiffs—who do not otherwise have privity of contract with Padlet and the choice-of-law provision in its terms—to bring their claims under California law.

21. **Divisional Assignment.** Pursuant to Civil Local Rules 3-2(c) and 3-5(b), assignment to the San Francisco or Oakland Division is proper because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in San Francisco County, where Padlet is headquartered, where it designed and developed the platform, where its decisions to deploy the challenged tracking technologies and to release the platform into the stream of commerce emanated, and where the majority of its U.S.-based employees work. Assignment to the San Francisco Division is also consistent with Padlet’s Terms of Service, which provide that any claim against Padlet “must be resolved exclusively by a state or federal court located in the City and County of San Francisco, California.”

III. THE PARTIES

22. Plaintiff M.C. 1 is a minor. At all relevant times, he has been a citizen of the state of Maryland. M.C. 1 attended school in a Maryland school district. As part of his schooling, he was required to access and use the Padlet Platform, which he accessed and used from his school-issued device.

23. Plaintiff M.C. 2 is a minor. At all relevant times, he has been a citizen of the state of Maryland. M.C. 2 attended school in a Maryland school district. As part of his schooling, he was required to access and use the Padlet Platform, which he accessed and used from his school-issued device.

24. Plaintiff Heidi Saas is the mother and legal guardian of Plaintiffs M.C. 1 and M.C. 2. At all relevant times, she has been a citizen of the state of Maryland.

⁴ *Open Roles*, Padlet, <https://padlet.jobs/open-roles> (last visited Aug. 31, 2026).

25. Defendant Wallwisher, Inc. d/b/a Padlet is a Delaware Corporation. Its headquarters are located at 981 Mission Street, San Francisco, California 94103.

IV. FACTUAL ALLEGATIONS

A. Padlet exploits education to collect and monetize students' PI.

26. Padlet's collection and dissemination of students' PI is a knowing and deliberate effort to exploit the economic reality that education is "the world's most data-mineable industry by far."⁵ The raw material being mined—students' PI—is shared and leveraged by third parties to fuel targeted marketing, behavioral prediction, and consumer profiling.⁶ These practices have generated massive private investment in EdTech⁷ businesses—\$16.1 billion in a single year⁸—and driven the industry's growth into a \$250 billion global market expected to nearly triple by 2027.⁹ It is this extraordinary commercial value, not any educational necessity, that motivates Padlet's collection and sharing of Plaintiffs' and students' PI essentially without guardrails.

27. Padlet markets and sells the Padlet Platform to K–12 schools and school districts. It provides digital bulletin boards and whiteboards for interactive instruction, classroom management, and assessment. The Padlet Platform was formerly called "Padlet Backpack" but was later rebranded as "Padlet for Schools." The Padlet Platform includes the following components:

- a. **Padlet Board** is a cloud-based digital bulletin board platform that allows students and teachers to add text, images, videos, audio, documents, and links to empty Boards or to

⁵ Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 15, 2014), <https://www.politico.com/story/2014/05/data-mining-your-children-106676>.

⁶ Hamed Ghorban Tanhaei, *Predictive analytics in customer behavior: Anticipating trends and preferences*, (Dec. 2024), <https://www.sciencedirect.com/science/article/pii/S2666720724000924>.

⁷ Although the term "educational technology" can be defined broadly to include purely theoretical or pedagogical practices, this Complaint uses "EdTech" to refer generally to "all the privately owned companies currently involved in the financing, production and distribution of commercial hardware, software, cultural goods, services and platforms for the educational market with the goal of turning a profit." *EdTech Inc.: Selling, Automating and Globalizing Higher Education in the Digital Age*, Tanner Mirrlees and Shahid Alvi (2019).

⁸ Alex Yelenevych, *The Future of EdTech*, Forbes (December 26, 2022), <https://www.forbes.com/councils/forbesbusinesscouncil/2022/12/26/the-future-of-edtech/?streamIndex=0>.

⁹ Louise Hooper, *et al.*, *Problems with Data Governance in UK Schools: the cases of Google Classroom and ClassDojo*, Digital Futures Commission, 5Rights Foundation (2022), <https://eprints.lse.ac.uk/119736/>.

1 featured templates for real-time collaboration with each other on lessons, assignments,
2 quizzes, and other classroom activities. Students and teachers can also share Boards
with each other and like, comment, and vote on each other's Boards.

3 **b. Padlet Sandbox** is a cloud-based digital canvas or whiteboard platform that allows
4 students and teachers to collaborate in real-time on lessons, presentations, assessments,
5 games, and a variety of other activities by adding text, images, videos, and other
multimedia content to the empty whiteboards or featured templates.

6 **c. Padlet TA** was an online AI-powered teaching assistant offered alongside the Board
7 and Sandbox components. It generated lessons, presentations, quizzes, and other
8 classroom activities to be presented within Padlet. Padlet discontinued Padlet TA on
9 June 30, 2026, stating that it "evolved into" **Padlet Arcade**, which is an AI-powered
game-creation platform.¹⁰ Padlet moved some of the non-game creation tools (tools for
the creation of worksheets, lesson plans, and presentations) to Gemini, where teachers
must log into Gemini for access.¹¹

10 28. By persuading schools to implement the Padlet Platform, Padlet gains virtually
11 unfettered access to the PI of the children who attend those schools, including Plaintiffs.

12 29. The Padlet Platform does not merely serve as a digital filing cabinet in which K–12
13 schools may store education records or locally stored digital workbooks. Rather, Padlet uses the
14 Padlet Platform to harvest students' PI and disseminate it freely to a broad and far-flung network
15 of third parties wholly unrelated to students' education. These functions are core to Padlet's
16 business model.

17 30. Given the significant value of student data in today's digital economy, several
18 investment firms have made substantial investments in Padlet, including Cherubic Ventures,
19 Y Combinator, Maverick Ventures, FundersClub, Bloomberg Beta, Burst Capital, and Maiden
20

21
22
23
24
25 ¹⁰ *Sunsetting Padlet TA*, Padlet Help, [https://padlet.help/1/en/article/10z0dbkbka-changes-to-](https://padlet.help/1/en/article/10z0dbkbka-changes-to-padlet-ta-content-creation-tools)
26 [padlet-ta-content-creation-tools](https://padlet.help/1/en/article/10z0dbkbka-changes-to-padlet-ta-content-creation-tools) (last visited Sept. 2, 2026); *Getting started with Padlet Arcade*,
Padlet Help, <https://padlet.help/1/en/article/52dhuz6x9b-getting-started-with-padlet-arcade> (last
27 visited Sept. 2, 2026).

28 ¹¹ *Sunsetting Padlet TA*, Padlet Help, [https://padlet.help/1/en/article/10z0dbkbka-changes-to-](https://padlet.help/1/en/article/10z0dbkbka-changes-to-padlet-ta-content-creation-tools)
[padlet-ta-content-creation-tools](https://padlet.help/1/en/article/10z0dbkbka-changes-to-padlet-ta-content-creation-tools) (last visited Sept. 2, 2026).

Lane.¹² At least seven private individuals have also invested in Padlet.¹³

31. Padlet has thus created a significant return for investors by taking and exploiting school-aged children's data at the expense of their privacy, including Plaintiffs' PI as described in this Complaint.

B. Padlet amasses a sweeping array of PI from student users of the Padlet Platform and exploits that PI for its own commercial gain and the profit of third parties.

1. Padlet admits to collecting a vast amount of PI from students.

32. Padlet admits to collecting a broad and detailed set of PI from students who use the Padlet Platform, including Plaintiffs and Class members.

33. Padlet collects at least the following PI from Plaintiffs and Class members who use the Padlet Platform:¹⁴

a. Student account and profile information:

- i. A student's full name;
- ii. A student's username;
- iii. A student's password;
- iv. A student's email address; and
- v. A student's profile photo.

b. Student-generated content on the Padlet Platform:

- i. Any text a student adds to the Padlet Platform;
- ii. Any images a student adds to the Padlet Platform;

¹² *Padlet Raises \$1.2 Million For Its Easy-To-Use, Collaborative Website Builder*, TechCrunch, <https://techcrunch.com/2015/09/18/padlet-raises-1-2-million-for-its-easy-to-use-collaborative-website-builder/> (Sept. 18, 2015) (last visited Sept. 2, 2026); *Portfolio*, Cherubic Ventures, <https://cherubic.com/company/> (last visited Sept. 2, 2026); *Maverick Ventures*, VC Sheet, <https://www.vcsheet.com/fund/maverick-ventures> (last visited Sept. 2, 2026); *Padlet Overview*, PitchBook, <https://pitchbook.com/profiles/company/55212-94#signals> (last visited Sept. 2, 2026); *Innovation – Bloomberg Beta*, Bloomberg, <https://www.bloomberg.com/company/values/tech-at-bloomberg/bloomberg-beta/> (last visited Sept. 2, 2026).

¹³ *Padlet Funding*, Wellfound, <https://wellfound.com/company/padlet/funding> (last visited Sept. 2, 2026).

¹⁴ *Privacy Policy*, Padlet, <https://legal.padlet.com/privacy#information-you-give-us> (last updated June 2, 2026) (accessed Sept. 2, 2026).

- iii. Any videos a student adds to the Padlet Platform;
- iv. Any audio a student adds to the Padlet Platform;
- v. Any documents a student adds to the Padlet Platform;
- vi. Any files a student adds to the Padlet Platform;
- vii. Any links from the Internet a student adds to the Padlet Platform;
- viii. Any drawings a student adds to the Padlet Platform; and
- ix. Any maps a student adds to the Padlet Platform.

c. **Precise student location information:** A student's precise-location information ("correct to 10 meters") when a student adds a map and allows location access.

d. **Student device information:**

- i. The brand, version, and type of a student's device;
- ii. The operating system and version of a student's device; and
- iii. The browser type and version of a student's device.

e. **Other student information:**

- i. A student's IP address;
- ii. A student's "content" and any content generated by a student;
- iii. "[I]nformation, including PI, about [a student] and how [the student] uses the [Padlet Platform]."
- iv. Any data collected about a student on other devices on which the student used or uses the Padlet Platform;
- v. Data from cookies stored on a student's devices when a student uses the Padlet Platform; and
- vi. "[G]eneral usage information" that may include the pages or features of the Padlet Platform visited by a student and the links within the Platform clicked on by a student.

2. Padlet admits to using students' PI for marketing and analytics.

34. Padlet admits that it uses PI for marketing and analytics and to improve and deliver

1 its products.¹⁵ Padlet’s use of PI for these purposes commercially benefits Padlet.

2 35. Padlet also purports to reserve an unlimited license to use PI, which includes
3 Plaintiffs’ and Class members’ PI, for its own benefit and without compensation to students.

4 36. Moreover, in its terms of service, Padlet purports to grant itself “a non-exclusive,
5 worldwide, royalty-free, sublicensable, transferable right and license to use, host, store, cache,
6 reproduce, publish, display (publicly or otherwise), perform (publicly or otherwise), distribute,
7 transmit, modify, adapt (including, without limitation, in order to conform it to the requirements of
8 any networks, devices, services, or media through which the Services are available)” any
9 “Subscriber Content” transferred to Padlet through Padlet’s services.¹⁶

10 37. Padlet also purports to grant itself the right to take and use “any idea, proposal,
11 suggestion or feedback, including technologies and product improvements” made by a user, stating
12 that the user “grant[s] to Padlet, without charge, royalties or other obligation to [the user], the right
13 to make, have made, create derivative works, use, share and commercialize that [f]eedback in any
14 way and for any purpose.”¹⁷

15 38. Padlet also enters into data-sharing agreements with third-party partners that
16 commercially benefit both Padlet and the third parties with which Padlet shares PI. The companies
17 all monetize the data in numerous ways, such as by using it to develop and enhance their own
18 products, facilitate greater data analytics and “user insights,” improve internal operations, or more
19 effectively target their marketing efforts and attract new customers. These types of indirect data
20 monetization can be at least as valuable to a company as directly monetizing it through the sale of
21 raw or aggregated data.

22 39. Padlet shares Plaintiffs’ and Class members’ PI for a host of commercial purposes,
23 enabling Padlet and third-party recipients to monetize that information.

24 40. Padlet refuses to disclose how it uses and shares the data of any individual student
25

26 ¹⁵ *Id.*

27 ¹⁶ *Terms of Service*, Padlet, <https://legal.padlet.com/terms> (updated May 6, 2026) (accessed
28 Sept. 2, 2026).

¹⁷ *Id.*

1 to the student or their parent, in violation of COPPA. *See* 16 CFR 312.3, 312.4, 312.5.

2 **3. Forensic analysis reveals that Padlet collects even more PI and shares students' PI**
 3 **with a myriad of AdTech companies in real time.**

4 41. Forensic analysis of the Padlet Platform reveals that Padlet collects even more PI
 5 about Plaintiffs and other students and transmits this PI to a multitude of AdTech companies in real
 6 time as they use the Padlet Platform, without the knowledge or consent of the students or their
 7 parents.

8 42. The categories of student information being recorded, duplicated, and transmitted to
 9 third-party companies, and the identity of the third parties with which that information is shared,
 10 are determined by the Padlet Platform and are typical of all student accounts and do not vary by
 11 user, their school, or their school district. In other words, every user of the Padlet Platform is subject
 12 to the same data practices regardless of their identity, school, or location.

13 **a. Padlet further expansively collects student PI.**

14 43. In addition to the categories of PI that Padlet admits to collecting as detailed
 15 above, forensic testing further confirms that Padlet collects and shares a broad range of persistent
 16 unique identifiers that are essentially linkage keys allowing children to be recognized repeatedly
 17 across sessions and devices

18 44. A “persistent unique identifier” is any a piece of information that (1) points *only* to
 19 an individual or an individual’s device, (2) will not change across multiple sessions, and (3) enables
 20 tracking over time. Persistent identifiers allow companies to track individuals’ interactions on
 21 websites or on internet-enabled devices over time, and to link each of those different interactions
 22 back to the same person. Examples of persistent unique identifiers include:

- 23 i. cookies (small text files that a website stores in your browser, used to keep you
 24 logged in, remember your preferences, track what pages you visit; *i.e.*, a cookie is
 25 like a note in your browser saying this is the same person who came here before);
- 26 ii. device fingerprints (a collection of technical details about your smartphone,
 27 computer, or other internet-enabled device such as browser version, screen size,
 28 settings, etc., that combine into a unique profile; *i.e.*, a device fingerprint is like

recognizing someone by their walk, voice, or clothing);

- iii. advertising IDs (identifying numbers assigned to your device by the operating system that gives advertisers a way to recognize that device to build a profile);
- iv. Universally Unique Identifiers (“UUIDs”) (a long randomly generated string designed to track and identify one specific user’s activity over time and across sessions and devices like smart phones, tablets, laptops, desktops and smart TVs; companies use UUIDs and persistent identifiers to build and grow a robust profile about the student, including, among many other things, where she lives, where she attends school, how well she performs academically, her behaviors, and her socioeconomic level); and
- v. Google advertising IDs (Google’s advertising and analytics systems’ way of recognizing the same user on different websites).

b. The PI taken by Padlet far exceeds “education records.”

45. The PI that Padlet extracts from Plaintiffs’ and Class members’ who use the Padlet Platform far exceeds what could be legally or traditionally characterized as “education records.”

46. Even if certain PI could be characterized as education records, all students retain significant rights over the PI contained in such records, which are protected by state and federal law.

47. Further, the amount of PI Padlet collects about children, including children under 13, far exceeds that reasonably necessary for children to participate in any school activity that is facilitated by the Padlet Platform, in violation of COPPA. *See* 16 CFR 312.7.

48. That the Padlet Platform is not designed to optimize for student privacy is an intentional, self-interested choice that comes at the expense of children’s privacy, safety, and autonomy.

c. Padlet knowingly exposes Plaintiffs’ and students’ PI to a staggering array of AdTech companies.

49. Forensic testing conducted on the Padlet Platform reveals that it captures and transmits Plaintiffs’ and Class members’ PI in real time to third-party AdTech companies that

1 include data brokers, identity-resolution companies, customer-data platforms, and other digital
2 advertising companies, without the knowledge or consent of the students or their parents.

3 50. A data broker is a business that collects and sells personal and sensitive consumer
4 information that the consumer did not give the broker directly.¹⁸ “Data brokers package, trade, and
5 sell information to various organizations, including ones [consumers have] never heard of
6 before.”¹⁹ Data brokers’ customers include advertising and marketing companies, employers and
7 recruiters, insurance companies, political campaigns, retail companies, landlords, debt collectors,
8 the U.S. military, federal law-enforcement agencies, and state and local law enforcement.²⁰

9 51. An identity-resolution company is a business that links and combines disparate
10 pieces of data about a person and the person’s behavior from different devices, websites, social-
11 media platforms, other online interactions, and data stored offline locally on a computer or server,
12 to provide a comprehensive profile of the person’s interactions and behaviors.²¹ The identity-
13 resolution companies store historical data about the person and continually collect new data and
14 update each profile accordingly.²²

15 52. A customer-data platform is a system that unifies customer profiles, provides
16 identity-resolution services, collects real-time data, and analyzes and activates all the data for
17 advertising, marketing, and analytics purposes.²³

18 **i. Forensic testing confirms Padlet knowingly shares Plaintiffs’ and**
19 **students’ PI to more than 160 third parties.**

20 ¹⁸ *Personal information and data brokers*, California Privacy Protection Agency,
21 <https://privacy.ca.gov/drop/personal-information-and-data-brokers/> (last visited Sept. 2, 2026).

22 ¹⁹ *Id.*

23 ²⁰ *Id.*; Will Greenberg, *How Ad Tech Became Cop Spy Tech*, Electronic Frontier Foundation
(Aug. 31, 2022) <https://www.eff.org/deeplinks/2022/08/how-ad-tech-became-cop-spy-tech> (last
visited Sept. 2, 2026).

24 ²¹ *The Ultimate Guide to Identity Resolution: What It Is, How It Works, Why It Matters*,
LiveRamp (March 31, 2026), [https://liveramp.com/blog/what-is-identity-
25 resolution#:~:text=Identity%20resolution%20is%20the%20process,without%20using%20third%
26 2Dparty%20cookies](https://liveramp.com/blog/what-is-identity-resolution#:~:text=Identity%20resolution%20is%20the%20process,without%20using%20third%2Dparty%20cookies) (last visited Sept. 2, 2026).

27 ²² *What Is Identity Resolution?*, TransUnion (Aug. 23, 2021),
<https://www.transunion.com/blog/what-is-identity-resolution> (last visited Sept. 2, 2026).

28 ²³ *What is a CDP?*, Microsoft (Nov. 1, 2025), [https://www.microsoft.com/en-us/dynamics-
365/resources/what-is-a-cdp](https://www.microsoft.com/en-us/dynamics-365/resources/what-is-a-cdp) (last visited Sept. 2, 2026).

1 53. The forensic testing reveals Padlet knowingly shared PI with over 160 third parties,
2 more than half of which were AdTech companies.

3 54. Of the AdTech companies receiving the PI, more than 40 were data brokers that
4 aggregate and sell PI, including LiveRamp, Nielsen Marketing (“Nielsen”), and TransUnion, some
5 of the largest brokers in the country. These companies all have massive consumer datasets that they
6 use and sell to other third parties for their own commercial benefit and the benefit of the third-party
7 recipients. Still other data brokers include Dotomi (part of data broker giant Epsilon, which also
8 operates as an identity-resolution company), MediaMath (now d/b/a Infillion), StackAdapt,
9 Zenlayer, and PulsePoint (specializing in healthcare data²⁴). Health information is particularly
10 sensitive PI, and there is no legitimate reason for Padlet to be disclosing any PI to any data broker,
11 much less to one that sells healthcare information.

12 55. Thirteen of the data brokers also operate as identity-resolution companies, including
13 LiveRamp, Nielsen, and TransUnion, meaning they not only collect and aggregate data from many
14 different online and offline sources, but they also use it to build robust profiles of each person and
15 then sell the data to a wide variety of third parties.

16 56. Testing further reveals Padlet sharing students’ PI with advertising companies,
17 including Integral Ad Science; Adkernel; Appier (also a customer-data platform and identity-
18 resolution company); MediaGo; Moloco; RocketFuel (now Zeta Global); Voise Tech; and Beamer
19 (a marketing and analytics company).

20 57. Padlet also shares PI with Meta Platforms (“Meta”) (the parent company of
21 Facebook and Instagram), which generates almost all of its revenue—more than \$196 billion in
22 2025—from advertising²⁵; and Google, the other largest digital advertiser in the country,
23 accounting for 26.4% of the total digital advertising revenue generated (compared to Meta’s 26.8%)
24

25 _____
26 ²⁴ *The Healthcare Marketing Platform*, PulsePoint, <https://www.pulsepoint.com/> (last visited
27 Sept. 2, 2026).

28 ²⁵ *Annual advertising revenue of Meta Platforms worldwide from 2009 to 2025*, STATISTA (Feb. 3,
2026), <https://www.statista.com/statistics/271258/facebook-advertising-revenue-worldwide/> (last
visited Sept. 2, 2026).

1 in the United States²⁶ (including Doubleclick, owned by Google and part of Google’s massive data
2 analytics and advertising ecosystem).

3 58. Specifically, where outbound traffic was observed from Padlet to third parties Meta
4 and Integral Ad Science (“IAS”), these companies returned tracking pixels, which are pieces of
5 code embedded in Padlet’s website to track students’ activity on Padlet and instantaneously send
6 PI to Meta and IAS for advertising and other purposes.²⁷

7 59. As the Federal Trade Commission explains, a tracking pixel is:

8 [A] small piece of code that will be placed into the website or ad and
9 define [the pixel operator’s] tracking goals such as purchases, clicks,
10 or pageviews. . . .

11 Pixel tracking can be monetized several ways. One way to monetize
12 pixel tracking is for companies to use the tracking data collected to
13 improve the company’s own marketing campaigns. . . . Another is
14 that companies can monetize the data collected by further optimizing
15 their own ad targeting systems and charging other companies to use
16 [their] advertising offerings.²⁸

17 60. Pixels collect a substantial amount of information regarding an individual’s online
18 behavior—the webpages viewed by the user, the amount of time spent by the user on specific
19 webpages, the buttons and hyperlinks that the user clicks while using a website, the text entered by
20 the user into a website search bar, and even the information provided by the user in an online form—
21 all transmitted in real-time as the user navigates a website.²⁹ Pixels also collect personal and
22 sensitive information about users.³⁰

23 ²⁶ *Meta to Surpass Google in Digital Ad Revenues For First Time Ever*, eMarketer (Apr. 13,
24 2026), <https://www.emarketer.com/press-releases/meta-to-surpass-google-in-digital-ad-revenues-for-first-time-ever/> (last visited Sept. 2, 2026).

25 ²⁷ *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION
26 – OFFICE OF TECHNOLOGY (Mar. 6, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking> (last visited Sept. 2, 2026).

27 ²⁸ *Id.*

28 ²⁹ *See id.*; *How does retargeting on Facebook help your business?*, META,
29 <https://www.facebook.com/business/goals/retargeting> (last visited Sept. 2, 2026); Tom Kemp,
30 “Oops! I Did It Again” ... Meta Pixel Still Hoovering Up Our Sensitive Data, MEDIUM,
31 https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47#_ftn1 (last visited Sept. 2, 2026).

32 ³⁰ *Id.*

61. Like Meta, Google receives students' PI from Padlet and returns tracking pixels that monitor students' activity while they use the Padlet Platform. However, Google's tracking differs in that its advertising IDs and pixel-matching technology are used to integrate students' Padlet classroom activity into Google's broader advertising and analytics ecosystem, enabling tracking and profiling of students across websites and devices beyond Padlet and beyond any one platform.³¹

62. The fact that student data, taken without consent while students are engaged in their compulsory education, is being shared, used, and sold in this way is deeply invasive and highly offensive. By doing so, Padlet forever makes children's private and sensitive information part of the public marketplace, enriches private businesses at children's expense, exposes their PI to misuse, and compromises the security of their PI.

ii. AdTech companies engage in mass advertising surveillance.

63. Many of the AdTech companies with which Padlet shares PI are part of what has become a mass advertising surveillance industry of tracking, collecting, and profiling people's online and offline activities for a wide variety of advertising purposes. None of the AdTech companies with which Padlet shares PI have any relation to the delivery of Padlet's purported educational services. They are all in the business of selling PI; analyzing, aggregating, and creating individual profiles based on PI for sale or use by themselves or other companies; using the PI to sell advertising services; or advertising.

64. Padlet has never disclosed that it shared PI with these companies.

65. For example, two of the scores of AdTech companies with which Padlet shares PI are online advertising and data-broker giants TransUnion and Epsilon. They are two of the largest data brokers, data analytics, and digital advertising companies in the country. Both companies have access to massive datasets from online and offline sources from which they compile as much information as possible about American consumers, including information relating to the most private aspects of their lives. They both also operate as identity-resolution companies, using their

³¹ *Google-initiated: Bidirectional Pixel Matching*, Google, <https://developers.google.com/authorized-buyers/rtb/cookie-guide#google-initiated:-bidirectional-pixel-matching> (last visited Sept. 2, 2026).

1 datasets to identify and build profiles of each individual consumer for their own use and for sale to
2 third-party buyers as fuel for a massive, targeted advertising enterprise.

3 66. TransUnion advertises its identity-resolution and data-analytics services to clients,
4 claiming the services create “a [t]ru[e] picture of each person: an actionable view of each consumer
5 based on a robust set of online, offline, public and proprietary information,” allowing business
6 clients to “[r]each and engage audiences seamlessly across all marketing channels” and
7 “[c]ontinuously measure and improve” their marketing.³²

8 67. Likewise, Epsilon touts that its “data assets” include data on 250 million U.S.
9 consumers and cover “virtually every marketable U.S. household.”³³ It further states that it “can
10 help [clients] efficiently identify and engage with [their] best and next-best customers with third-
11 party data.”³⁴

12 68. Yet another data broker with which Padlet was seen sharing PI in forensic testing is
13 Pulsepoint, which specializes in healthcare data. Pulsepoint states that it “see[s] 92% of the U.S.
14 population” and reaches “more than 95% of healthcare professionals.”³⁵ Pulsepoint further states
15 that it “unifies digital determinants of health and real-world data to produce the most dimensional
16 view of the health customer.”³⁶

17
18
19 [Remainder of page intentionally left blank]
20
21
22

23 ³² *About TransUnion*, TransUnion, <https://www.transunion.com/about-us> (last visited Sept. 2,
24 2026); *TruAudience*, TransUnion, <https://www.transunion.com/solution/trueaudience> (last visited
25 Sept. 2, 2026).

26 ³³ *Data*, Epsilon, <https://www.epsilon.com/us/products-and-services/data> (last visited Sept. 2,
27 2026).

28 ³⁴ *Id.*

³⁵ *Healthcare Marketing Technology Built for Precision and Scale*, PulsePoint, <https://www.pulsepoint.com/healthcare-marketing-activation> (last visited Sept. 2, 2026).

³⁶ *The Healthcare Marketing Platform*, PulsePoint, <https://www.pulsepoint.com/> (last visited Sept. 2, 2026).

69. The AdTech companies aggregate information that they collect from third-party websites into “advertising profiles” consisting of all data that they have collected about a user.³⁷

70. With these advertising profiles, the AdTech companies can sell hyper-precise advertising services, allowing their clients to target internet users based on combinations of their location, age, race, interests, hobbies, education level, use of specific apps or websites, and more.³⁸

71. For example, some of the profile information Epsilon claims it can provide to clients includes information about each person’s demographics, lifestyle, health and wellness, finances and wealth, purchase history, propensity to buy certain products or donate to certain causes, “attitudes,” and shopping preferences.³⁹

72. Because Padlet does not disclose that it shares PI with TransUnion, Epsilon, PulsePoint, and a multitude of other AdTech companies, Plaintiffs and Class members could not have been reasonably expected to review any of the AdTech companies’ privacy statements in connection with their use of the Padlet Platform.

73. This sweeping, invasive surveillance of Americans’ internet usage and resulting violation of their privacy is not accidental. Google’s former CEO, Eric Schmidt, admitted in 2010:

³⁷ *Id.* (“With our consumer data, you’ll learn who this person is, what they buy and what they care about.”); *Bring Clarity to Chaos*, TransUnion, <https://www.transunion.com/solution/trueaudience/clarity> (“Get a deep, 360-degree view of your customers, bringing together thousands of different data points into a single unified profile.”) (last visited Sept. 2, 2026); *The Healthcare Marketing Platform*, PulsePoint, <https://www.pulsepoint.com/> (“PulsePoint unifies digital determinants of health and real-world data to produce the most dimensional view of the health customer.”) (last visited Sept. 2, 2026); Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (2019), available online at: https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf.

³⁸ *Insights Solutions*, TransUnion, <https://www.transunion.com/solution/trueaudience/marketing-insights> (“Understand consumers based on 172 granular segments and demographic, behavioral, property, financial and geographic data.”) (last visited Sept. 2, 2026); *What is Customer Intelligence (CI)? Examples & Insights*, LiveRamp, <https://liveramp.com/blog/what-is-customer-intelligence-ci-examples-insights#:~:text=Demographic%20Data,targeting%2C%20and%20measurement%20of%20campaigns>. (last visited Sept. 2, 2026).

³⁹ *Id.*

1 “We know where you are. We know where you’ve been. We can more or less know what you’re
2 thinking about.”⁴⁰

3 **C. Plaintiffs are among the students whose PI is extracted, used, and shared by Padlet.**

4 74. Plaintiffs are among the students whose PI Padlet has continuously taken, used, and
5 shared with AdTech companies without consent.

6 75. Both M.C. 1 and M.C. 2 have used and continue to use the Padlet Platform in their
7 schools as part of their required curriculum. They both have completed lessons, assignments,
8 games, and other classroom activities within the Padlet Platform.

9 76. M.C. 1 used the Platform throughout his sixth-grade year (2024–2025) when he was
10 twelve years old, and in his seventh-grade year (2025–2026) at age 13.

11 77. M.C. 2 used the Padlet Platform throughout his sixth-grade school year
12 (2025–2026).

13 78. School personnel created the Padlet Platform accounts for M.C. 1 and M.C. 2.
14 Neither Plaintiffs nor their parents were provided with any terms or policies pertaining to the Padlet
15 Platform, nor were they provided an opportunity to withhold consent to Padlet’s data practices.

16 79. When M.C. 1 and M.C. 2 completed their required lessons, assignments, and other
17 classroom activities in the Padlet Platform, Padlet extracted their highly sensitive, private, and
18 personal PI, including their demographic data; content they created; text files they uploaded; their
19 use of the built-in camera, video recorder, and audio recorder; their comments to teachers and other
20 students; and their search terms and links clicked while using the Internet, YouTube, Spotify and
21 other online databases to which Padlet provides built-in links.

22 80. Padlet has thus collected vast troves of demographic, academic, and behavioral data
23 belonging to M.C. 1 and M.C. 2, including their PI, through their use of the Padlet Platform.

24 81. While Plaintiffs used the Padlet Platform, Padlet shared their PI with myriad
25 AdTech companies as detailed above.

26 82. Neither Plaintiffs nor their parents consented to Padlet’s collection or sharing of

27 ⁴⁰ Andrew Orlovski, *Google’s Schmidt: We know what you’re thinking*, THE REGISTER (Oct. 4,
28 2020), https://www.theregister.com/2010/10/04/google_ericsms/ (last visited Sept. 2, 2026).

1 Plaintiffs' PI.

2 83. Ms. Saas requested access to M.C. 1's and M.C. 2's data from Padlet when they
3 were both under 13, but Padlet denied her request, instead referring her to her school district, in
4 violation of COPPA. *See* 16 CFR 312.3, 312.6.

5 84. After the school district later instructed Padlet to release the data to Ms. Saas, Padlet
6 did not do so and, to date, has not done so or otherwise further communicated with Ms. Saas.

7 85. Padlet has a policy and practice of denying Parents access to information about their
8 children to which they are entitled in violation of federal law.

9 86. Consequently, students and parents do not and cannot know the full extent of the PI
10 Padlet collects from them, whether that data is accurate, how that data is stored, how long that data
11 is retained, who has accessed that data, or how that data or data-derivative information or products
12 are used by Padlet or third parties.

13 **D. Padlet fails to obtain effective consent for its sweeping extraction, use, and disclosure**
14 **of Plaintiffs' and Class members' PI**

15 87. A party seeking to raise consent as a defense to alleged tortious conduct has the
16 burden of proving that it obtained effective consent.

17 88. Effective consent may be express or implied, but it must be actual.

18 89. Before collecting, using, and sharing Plaintiffs' and Class members' PI, Padlet fails
19 to obtain informed, voluntary consent from a person with authority.

20 90. Specifically, any purported consent obtained by Padlet is ineffective because
21 (1) Padlet both fails to provide its terms and policies to parents and fails to disclose sufficient
22 information about its data practices to support informed consent; (2) student use of the Padlet
23 Platform is not voluntary; and (3) such consent is not obtained from a person with authority to
24 provide consent to Padlet's collection, use and disclosure of student information.

25 **1. Any purported consent was not informed.**

26 91. For consent to be effective, it must be informed, meaning the aggrieved person must
27 have sufficient knowledge of the nature of the act or transaction to make an educated decision.
28

1 92. Further, before collecting PI from children under 13, COPPA requires a company to
2 provide parental notice of its data practices that is “clearly and understandably written, complete”
3 and contains “no unrelated, confusing, or contradictory materials.” *See* 16 CFR 312.4(a).

4 93. Padlet does not provide students or their parents any notice of its data practices
5 before collecting PI.

6 94. Students do not create their Padlet accounts; school personnel do.

7 95. Padlet also does not provide the terms and policies that govern its data practices to
8 students or parents.

9 96. Thus, none of Plaintiffs, Class members, or their parents, received any information
10 necessary to support informed consent.

11 97. Even if Padlet had provided Plaintiffs’ and Class members’ parents its terms and
12 policies, Plaintiffs’ and Class members’ parents would not have been able to understand them
13 because they offer only general, vague statements with very little specific information or details or
14 entirely omit disclosures about Padlet’s actual data practices.⁴¹ For example, Padlet states that it
15 “may share aggregated information . . . and other de-identified or non-personally identifiable
16 information, with partners, press, or other third-parties in order to, for example demonstrate how
17 Padlet is used, spot industry trends, or to provide marketing materials for Padlet.”⁴² Padlet does not
18 define or provide any details or specific information about which information is shared or the
19 “partners, press, or other third-parties” to which Padlet sends the information.⁴³ Padlet’s terms and
20 policies also wholly fail to disclose the multitude of data brokers and other advertising companies
21 with which Padlet shares PI, as detailed above.

22 98. Therefore, even if a parent was notified that their child would be using the Padlet
23 Platform at school, it would be impossible for that parent to understand its data practices as

24 _____
25 ⁴¹ *Terms of Service*, Padlet, <https://legal.padlet.com/terms> (last updated May 6, 2026) (last visited
26 Sept. 2, 2026); *Privacy Policy*, Padlet, <https://legal.padlet.com/privacy> (last updated June 2, 2026)
27 last visited Sept. 2, 2026); *GDPR*, Padlet, <https://legal.padlet.com/gdpr> (last updated Mar. 23,
28 2026) (last visited Sept. 2, 2026).

⁴² *Privacy Policy*, Padlet, [https://legal.padlet.com/privacy#whom-do-we-share-the-collected-
information-with](https://legal.padlet.com/privacy#whom-do-we-share-the-collected-information-with) (last updated June 2, 2026) (last visited Sept. 2, 2026).

⁴³ *Id.*

1 necessary to support informed consent to those practices on behalf of their child.

2 **2. Any purported consent was not voluntary.**

3 99. For consent to be effective, it must be freely given.

4 100. Every state has compulsory education laws.

5 101. Schools use the Padlet Platform to support a host of pedagogical and administrative
6 functions.

7 102. Students whose schools use the Padlet Platform are required to use it. Parents are
8 not asked for permission for their children to use the Padlet Platform, nor are they given an
9 opportunity to refuse to consent to Padlet's data practices.

10 103. Further, Padlet may not place students and their parents in the position of having to
11 choose between their right to privacy and their right to an education. Nor may Padlet place students
12 and their parents at risk of compromising their relationship with their teachers and school
13 administrators or the quality of the education their children receive. Such inherently coercive
14 circumstances do not support freely given consent: to be effective, consent must be as easy to
15 withhold or revoke as it is to provide.

16 104. Use of the Padlet Platform under these circumstances would not lead a reasonable
17 person to believe that a student or their Parent had freely consented to Padlet's data practices.

18 **3. Any purported consent was not obtained by a person with authority.**

19 105. A party seeking to raise consent as a defense to alleged tortious conduct has the
20 burden of proving that it obtained effective consent.

21 106. For consent to be effective, it must be obtained from the aggrieved person or a
22 person authorized to consent on their behalf. For minors, that is a parent.

23 107. In addition to general consent requirements, COPPA contains heightened parental-
24 consent requirements that Padlet must meet before it may collect, use, or share PI from children
25 under 13. Specifically, COPPA requires that Padlet provide parents notice that is clearly and
26 understandably written, complete, and contains no unrelated, confusing, or contradictory materials,
27 including a list of specific notice requirements with which Padlet does not comply.
28

1 See 16 CFR 312.4(a). COPPA further requires the company to “obtain verifiable parental consent
2 before any collection, use, or disclosure of PI from children, including consent to any material
3 change in the collection, use, or disclosure practices to which the Parent has previously consented.”

4 See 16 CFR 312.3, 312.4, and 312.5.

5 108. Padlet has never obtained, and does not purport to obtain, consent from students or
6 their parents before it takes, uses, and shares students’ PI, including that of Plaintiffs and Class
7 members. Nor does it comply with heightened notice-and-consent requirements of COPPA.

8 109. Instead, Padlet relies on the consent of schools alone.

9 110. No personnel at Plaintiffs’ school had authority to consent to Padlet’s data practices
10 on students’ behalf in lieu of their parents.

11 111. School personnel are not legal guardians of Plaintiffs and Class members.

12 112. Plaintiffs’ and Class members’ schools do not own Plaintiffs’ and Class members’
13 PI.

14 113. Plaintiffs and Class members have significant privacy and property rights in their
15 own PI.

16 114. Plaintiffs’ and Class members’ schools could not and cannot legally consent—in
17 lieu of Plaintiffs or Class members or over their objections—to the disclosure of their PI by Padlet,
18 even if such disclosure may confer a benefit upon schools that is administrative, pedagogical, or
19 otherwise, or even upon students themselves.

20 115. Plaintiffs’ and Class members’ schools do not control the generation, collection,
21 storage, use, or disclosure of Plaintiffs’ and Class members’ PI by Padlet or any third party to which
22 Padlet grants access to Plaintiffs’ and Class members’ PI.

23 116. Padlet does not require or obtain proof that students or parents have authorized their
24 respective schools to act as their agent or intermediary to provide consent on their behalf.

25 117. Padlet does not require or obtain proof that Plaintiffs and Class members authorized
26 their respective schools to consent on their behalf as their agent or intermediary, and Plaintiffs and
27 Class members do not provide any such authorization.

118. Padlet has thus generated, collected, used, and disclosed Plaintiffs' PI to third parties without effective consent, and it continues to do so.

E. Padlet makes false and misleading statements about its data practices.

119. Padlet makes false and misleading statements about its data practices and the law on which it intends school personnel to rely to avoid seeking parental consent and to keep parents in the dark.

1. Padlet falsely states that schools, not Padlet and other EdTech companies, are responsible for complying with the consent requirements of COPPA.

120. In its Terms of Service, Padlet falsely states that a school "sponsor" or the school itself "assumes the responsibility for complying with COPPA[.]"⁴⁴

121. Padlet further falsely states that the school "[s]ponsor must notify parents/guardians of the information to be collected and obtain parental/guardian consent before collecting and sharing with [Padlet] the PI of children under the age of 13[.]"⁴⁵

122. In fact, COPPA in no way governs schools. COPPA is silent as to schools. *See generally*, 15 U.S.C. § 6501, *et seq.*; 16 CFR Part 312, *et seq.* Rather, COPPA expressly governs private companies like Padlet, and that law requires companies like Padlet to obtain parental consent before taking, using, or sharing the PI of children under 13. *See id.*

123. By falsely characterizing COPPA as placing the duty of compliance on schools, Padlet attempts to mask its own non-compliance with COPPA. Specifically, Padlet violates numerous provisions of COPPA. With respect to children under 13, Padlet:

- a. fails to provide parents with complete, understandable notice of its data practices, including when its terms and policies materially change, *see* 16 CFR 312.3, 312.4, and 312.5.;
- b. fails to obtain verifiable parental consent before taking, using, and disclosing children's PI, *see id.*;
- c. fails to provide parents access to and control over their children's PI or explain

⁴⁴ *Terms of Service*, Padlet, <https://legal.padlet.com/gdpr> (last updated May 6, 2026)

⁴⁵ *Id.*

1 how that information has been used and shared, *see* 16 CFR 312.3 and 312.6.;

2 d. collects far more information than is necessary for student participation in school
3 activities, *see* 16 CFR 312.7; and

4 e. retains student information for longer than permitted, *see* 16 CFR 312.8 and
5 312.10.

6 124. Padlet intends that school personnel rely on its false statements to avoid seeking
7 parental consent and parental scrutiny.

8 **2. Padlet falsely states that schools may use the Padlet Platform in compliance with**
9 **FERPA.**

10 125. Padlet falsely states that it complies with FERPA.⁴⁶ *See* 20 U.S.C. § 1232g, *et seq.*;
11 34 CFR 99, *et seq.*

12 126. Padlet further falsely states that a school sponsor or the school itself “represent[s]
13 and warrant[s] that [they] have the proper authority to designate and, as a result of engaging with
14 the Padlet Services do hereby designate, Padlet a ‘school official’ within the meaning of FERPA.”⁴⁷

15 127. In fact, Padlet’s data practices do not comply with FERPA, which requires that
16 schools obtain parental consent before disclosing certain student information to any third party. *See*
17 34 CFR § 99.30. The “school official” exception to this requirement permits a school to release
18 “education records” to “other school officials” under limited circumstances: the “school official”
19 must (1) perform an institutional service or function for which the school would otherwise use
20 employees; (2) be under the direct control of the school as to the use and maintenance of education
21 records; and (3) not redisclose any personally identifiable information from education records
22 without prior parental consent. *See* 34 CFR § 99.31.

23 128. The school-official exception does not absolve Padlet of its duty to obtain parental
24 consent before generating, collecting, using, or disclosing PI for numerous reasons:

25 _____
26 ⁴⁶ *Peace of mind for administrators*, Padlet, https://padlet.com/site/education#:~:text=Avoid%20technology%20overload,@shiv_teaching
27 (last visited Sept. 2, 2026).

28 ⁴⁷ *Terms of Service*, Padlet, <https://legal.padlet.com/terms> (last updated May 6, 2026) (last visited Sept. 2, 2026).

- a. FERPA regulates schools, not private companies;
- b. Padlet generates and takes PI directly from students;
- c. Padlet’s data practices are not directly controlled by schools;
- d. Padlet obtains information far beyond “education records”;
- e. Padlet uses data for commercial purposes; and
- f. Padlet rediscloses student information to numerous third parties without first obtaining parental consent.

129. Further, students retain significant, legally protected privacy interests in their PI contained within education records, including those disclosed by schools to third parties under the school-official exception.

3. Padlet makes false statements and misrepresentations about its use and disclosure of students’ data.

130. Padlet falsely states that student “data is never monetized or shared for advertising purposes” and that Padlet “ha[s] not shared [students’] PI with any third party for direct marketing purposes.”⁴⁸

131. As discussed above, Padlet *immediately* shares Plaintiffs’ and Class members’ PI with numerous data brokers, identity-resolution companies, and other AdTech companies.

132. Padlet also states that its “business model is not based on ads” and that it “do[es] not use [students’] data to serve targeted advertisements.”⁴⁹

133. Padlet deliberately misleads Plaintiffs and Class members and their parents by claiming—explicitly or by omission—that students are not subjected to advertising-driven data practices, while concealing that it routinely shares students’ personal information with a vast network of third-party companies that use that data to profile students and target them for advertising and other commercial purposes.

⁴⁸ *Terms of Service*, Padlet, <https://legal.padlet.com/terms> (last updated May 6, 2026) (last visited Sept. 2, 2026); *Privacy Policy*, Padlet, <https://legal.padlet.com/privacy> (last updated June 2, 2026) (last visited Sept. 2, 2026).

⁴⁹ *GDPR*, Padlet, <https://legal.padlet.com/gdpr> (last updated Mar. 23, 2026) (last visited Sept. 2, 2026).

134. Padlet further falsely states that the Padlet Platform is “private” and “secure.” As detailed above, the Padlet Platform is anything but private and secure, as it allows teachers and student users to embed multimedia content from the open internet into the Padlet Platform and continuously feeds students’ PI to AdTech companies and a host of other third parties.

4. Padlet falsely states that it provides parents access to their children’s data collected by Padlet.

135. Padlet falsely states that “[u]sers can request detailed information about the data [Padlet] hold[s] on them, and [Padlet] provide[s] it in a structured, commonly used, and machine-readable format.”⁵⁰

136. Indeed, Padlet has a policy and practice of denying parents access to their children’s information, as discussed above with respect to Plaintiffs.

137. Padlet intends that schools rely on its false statements to avoid seeking parental consent and parental scrutiny.

F. Padlet’s nonconsensual data practices harm students.

138. Padlet’s surreptitious data practices are not benign. Rather, they harm Plaintiffs and Class members in myriad ways that are immediate, long-lasting, and substantial.

1. Padlet harms children by invading their privacy.

139. A person’s right to privacy begins with protection from having information created about them in the first instance.

140. The right to privacy encompasses the person’s right to control information concerning his or her person. Loss of such control harms a person’s ability to, for example, manage and minimize risk.

141. Padlet’s data practices violate children’s fundamental right to privacy. They forever wrest from children and their parents control over Plaintiffs’ and Class members’ PI, including the right to determine whether such information is created in the first place.

142. Padlet collects, uses and discloses PI about school-aged children—for the

⁵⁰ *Id.*

1 commercial benefit of itself and numerous third parties—from data it takes from students while
2 they use the Padlet Platform as part of their legally required education.

3 143. Padlet also knowingly shares students’ PI with data brokers and other AdTech
4 companies that use the information to build profiles on the children and target them for advertising
5 or other purposes.

6 144. That Padlet targets minors in a compulsory environment and without parental notice
7 or consent is conduct that is highly offensive to a reasonable person and constitutes an egregious
8 breach of social norms.

9 **2. Padlet harms children by compromising the security of their PI.**

10 145. By collecting, storing, and sharing Plaintiffs’ and Class members’ PI, Padlet forever
11 jeopardizes that information by making it vulnerable to a host of data security risks.

12 146. Rates of cybercrime are steadily rising, including numerous data breaches that affect
13 a host of consumers and their PI, and education is a high-priority target.

14 147. Schools and school districts have been particularly and increasingly targeted by
15 cybercriminals in recent years, resulting in leaks of highly personal information about children that
16 was sometimes even made publicly available.

17 148. For example, one widely used EdTech company was hacked twice within a two-
18 week span in May 2026. A criminal-extortion group took credit and, after the first hack, threatened
19 that if the company did not pay a ransom, the group would leak “[s]everal billion . . . private
20 messages among students and teachers and students and other students involved, containing
21 personal conversations and other [personally identifiable information].”⁵¹ The EdTech company
22 acknowledged in a public statement that the stolen data included identifying information “such as
23 names, email addresses, and student ID numbers, as well as messages among users.”⁵²

24 149. When the company did not cooperate with the criminal group, the group hacked it a

25 _____
26 ⁵¹ *‘PAY OR LEAK’: Hackers Target Big Higher Ed Vendor*, Higher Ed News (May 5, 2026),
27 available at [https://www.insidehighered.com/news/tech-innovation/administrative-](https://www.insidehighered.com/news/tech-innovation/administrative-tech/2026/05/05/pay-or-leak-hackers-target-big-higher-ed-vendor)
28 [tech/2026/05/05/pay-or-leak-hackers-target-big-higher-ed-vendor](https://www.insidehighered.com/news/tech-innovation/administrative-tech/2026/05/05/pay-or-leak-hackers-target-big-higher-ed-vendor) (last accessed Sept. 2, 2026).

⁵² *Confirmed Security Incident*, Instructure, https://www.instructure.com/incident_update
(updated July 21, 2026) (last accessed Sept. 2, 2026).

second time, obtaining more data and disrupting teachers’ and students’ access to the company’s services in schools throughout the country.⁵³ The company then announced that it “reached an agreement with the unauthorized actor involved in th[e] incident” and claimed that the data was returned and destroyed and that the criminal group claimed it would not extort individual customers.⁵⁴

150. When companies pay ransoms to hackers, they encourage more hackers to follow suit. Indeed, the FBI “does not support paying a ransom” because it “doesn’t guarantee you . . . will get any data back” and “encourages perpetrators to target more victims and offers an incentive for others to get involved in [it].”⁵⁵

151. The same criminal group involved in the May 2026 attacks also hacked another EdTech company only two months before that, in March 2026.⁵⁶ The company acknowledged the breach and ransom demand but claimed the stolen data was that of school staff members and not students.⁵⁷ A third EdTech company was hacked and subject to a ransom demand in December 2024, compromising the personal information of tens of millions of students dating back four decades.⁵⁸ The hacker in that case was a college student who stated after his arrest that “it’s easy, easy money” and that he was “thankful for [the FBI] . . . because [he] would have never

⁵³ *What we know about the Canvas hack that has impacted thousands of schools*, CNN, <https://www.cnn.com/2026/05/07/us/canvas-hack-strands-college-students-finals-week> (last visited Sept. 2, 2026).

⁵⁴ *Security Incident Update & FAQs*, Instructure, https://www.instructure.com/incident_update (last visited Sept. 2, 2026).

⁵⁵ *How We Can Help You*, FBI.gov, <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware> (last visited Sept. 2, 2026).

⁵⁶ *School software serving 11M students hacked, ShinyHunters claims attack*, cybernews, <https://cybernews.com/security/software-11m-students-hacked-shinyhunters-attack/> (last visited Sept. 2, 2026).

⁵⁷ *Notice regarding a security incident*, Infinite Campus, https://content.govdelivery.com/attachments/NCSBE/2026/03/23/file_attachments/3591917/InfiniteCampusMarch22_note.PNG.pdf (last visited Sept. 2, 2026).

⁵⁸ *Malware stole internal PowerSchool passwords from engineer’s hacked computer*, TechCrunch, <https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/> (last visited Sept. 2, 2026).

1 stopped.”⁵⁹

2 152. Educational data is also a high-priority target for nation-state threat actors. A
3 Microsoft 2024 Digital Defense Report found that the education and research sector was the
4 second-most targeted sector by nation-state threat actors from Russia, China, Iran, and North
5 Korea.⁶⁰

6 153. Such exposure can have immediate and long-term consequences for children. As
7 explained by one cybersecurity professional whose son’s school was hacked, “It’s your future. It’s
8 getting into college, getting a job. It’s everything.”⁶¹ Regarding the 2024 EdTech data breach, a
9 former FBI official said that “[i]t was one of the worst I’ve seen here when you talk about financial
10 impact. You talk about the forever impact that these students and faculty will have for the rest of
11 their lives.”⁶²

12 154. Padlet’s sweeping, invasive, and indiscriminate data practices unduly compromise
13 the security of children’s personal and private information.

14 155. Plaintiffs’ and Class members’ PI is further compromised by Padlet’s practice of
15 sharing that PI with a multitude of third parties. And the resulting harms and risks of harms are
16 exacerbated by the sheer volume of data collected and the number of entities that receive access to
17 it. Once such data is unlawfully obtained, the harms are irreversible.

18 156. In sum, Padlet’s data practices harm children from the moment their PI is obtained
19

20 ⁵⁹ *College student who hacked PowerSchool software says he’s grateful he was caught*,
21 WMRU9abc, <https://www.wmur.com/article/college-student-hack-powerschool-41426/71017881>
(last visited Sept. 2, 2026).

22 ⁶⁰ *Microsoft Digital Defense Report 2024*, Microsoft, <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024> (last visited
23 Sept. 2, 2026).

24 ⁶¹ Natasha Singer, *A Cyberattack Illuminates the Shaky State of Student Privacy*, The New York
25 Times (July 31, 2022), <https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html> (last visited Sept. 2, 2026).

26 ⁶² “*I was addicted to hacking*”: Teen tells how gaming led to cybercrime, breaching nationwide
27 school systems, including Texas, WFAA ABC News,
28 <https://www.wfaa.com/article/news/crime/teen-tells-how-gaming-led-to-cybercrime-breaching-nationwide-school-systems-including-texas/287-1fcef3dc-f067-4de4-8c06-10bac85ce180> (last visited Sept. 2, 2026).

by Padlet.

157. That harm is exacerbated by Padlet's persistent storage, use, and disclosure of that information to its vast network of partners and other third parties.

3. Padlet harms children by forcing them to choose between their right to an education and other fundamental rights.

158. Padlet forces Plaintiffs and Class members into the untenable position of having to choose between their right to an education and other fundamental rights, such as their rights to privacy and property.

159. Research shows that nearly 80% of adults reported being very or somewhat concerned about how companies use data collected about adults,⁶³ and the number of those concerned about their online privacy is growing quickly.

160. Protective behaviors are on the rise, with 87% of U.S. adults using at least one privacy- or security-protecting tool online.⁶⁴

161. An even greater percentage of parents value protecting their children's PI, including their identity (90%), location (88%), health data (87%), age (85%), school records (85%), and browsing history (84%).⁶⁵

162. Padlet has driven a wedge between school personnel and Plaintiffs' and Class members' parents, leaving parents reluctant to press their schools for information regarding Padlet's data practices or request that their children be alternatively accommodated.

163. Parents fear becoming adversarial with their children's schools and the possible repercussions they or their children might suffer if they are perceived as difficult or meddlesome, including stigmatization or retaliation. Padlet has thus chilled parental efforts to inquire about and

⁶³ Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> (last visited Sept. 2, 2026).

⁶⁴ Olivia Sideot and Emily Vogels, *What Americans Know About AI, Cybersecurity and Big Tech*, Pew Research Center (August 17, 2023), <https://www.pewresearch.org/internet/2023/08/17/what-americans-know-about-ai-cybersecurity-and-big-tech/> (last visited Sept. 2, 2026)..

⁶⁵ *Polling Memo: Parents' Views on Children's Digital Privacy and Safety*, Trusted Future (2022), <https://trustedfuture.org/childrens-digital-privacy-and-safety/> (last visited Sept. 2, 2026).

object to its practices.

164. This chilling effect has left children particularly vulnerable and disempowered to protect themselves against Padlet’s exploitative conduct.

G. Padlet’s nonconsensual data practices are unfair and unlawful.

165. Padlet has generated profits through its collection of children’s PI—without their parents’ knowledge or consent, and without compensating them for actively and passively providing Padlet with valuable information.

166. This one-sided arrangement—whereby Padlet generates profits each year using the PI of children gathered through children’s compelled use of the Padlet Platform, and all that children receive in return are education services to which they are already legally entitled—is particularly unjust given the core philanthropic purpose and compulsory nature of a public education.

167. Through its surreptitious, exploitative data practices, Padlet has unjustly enriched itself at the cost of children’s privacy, security, and autonomy, when children would otherwise have the ability to choose how they would monetize their data—or decide not to. School-aged children should not be made to bear these risks and harms for the commercial benefit of private, for-profit corporations like Padlet and its partners.

V. CLASS ACTION ALLEGATIONS

168. Plaintiffs bring this class action pursuant to Rules 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure on behalf of themselves and all other similarly situated.

169. Plaintiffs seek to represent a nationwide class of students (“Nationwide Class”) defined as:

All persons in the United States who attend or attended a K–12 school who used the Padlet Platform.

170. Plaintiffs also seek to represent a state-only subclass of students (“Maryland Subclass”) under the laws of the State of Maryland defined as:

1 *All persons in Maryland who attend or attended a K–12 school who*
2 *used the Padlet Platform.*

3 171. In addition, and in the alternative to the Nationwide Class, Plaintiffs reserve the right
4 to seek leave to amend the complaint to represent multi-state and individual state subclasses under
5 the laws of 50 states.

6 172. Plaintiffs reserve the right to modify or amend the definition of the proposed classes
7 before the Court determines whether certification is appropriate.

8 173. The Nationwide Class and Maryland Subclass are collectively referred to herein as
9 the “Classes.” Members of both Classes are collectively referred to herein as “Class members.”

10 174. Excluded from the Classes are: (1) the Court (including any Judge or Magistrate
11 presiding over this action and any members of their chambers and families); (2) Padlet, its
12 subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of
13 them have a controlling interest and its officers, directors, employees, affiliates, or legal
14 representatives; (3) persons who properly and timely request exclusion from the Classes;
15 (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise
16 released; (5) Plaintiffs’ counsel, Classes’ members counsel, and Padlet’s counsel; and (6) the legal
17 representatives, successors, and assigns of any such excluded person.

18 175. **Ascertainability:** Membership of the Classes is defined based on objective criteria
19 and individual members will be identifiable from Padlet’s records, including from Padlet’s massive
20 data storage. Based on information readily accessible to it, Padlet can identify Class members who
21 have used the Padlet Platform.

22 176. **Numerosity:** Class members are so numerous that joinder of all members is
23 impracticable. The exact size of the Classes and the identities of the Class members are readily
24 ascertainable in or through Padlet’s records.

25 177. **Typicality:** Plaintiffs’ claims are typical of the claims of other Class members, as
26 all Class members were uniformly affected by Padlet’s wrongful conduct in violation of federal
27 and state law as described herein.
28

1 178. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Class
2 members and have retained counsel that is competent and experienced in class action litigation,
3 including nationwide class actions and privacy violations. Plaintiffs and their counsel have no
4 interest that is in conflict with or otherwise antagonistic to the interests of the other Class members.
5 Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the
6 Class members, and they have the resources to do so.

7 179. **Commonality:** Common questions of law and fact exist as to all Class members
8 and predominate over any questions affecting solely individual Class members. Common questions
9 for the Classes include, but are not limited to, the following:

- 10 a. Whether Padlet obtained effective consent to generate, obtain, use, and disclose the
11 personal and private information of the Class members;
- 12 b. Whether Padlet led the Class members to believe, either directly or through school
13 personnel, that their data and their privacy would be protected;
- 14 c. Whether Padlet represented that Class members could control what data were
15 intercepted, received, collected, or shared by Padlet;
- 16 d. Whether Padlet actually protected the data and privacy of Class members;
- 17 e. Whether Padlet's practice of intercepting, receiving, collecting, or sharing users' data
18 violated state or federal privacy laws;
- 19 f. Whether Padlet's practice of intercepting, receiving, collecting, or sharing users' data
20 violated any other state or federal tort laws;
- 21 g. Whether Plaintiffs and Class members are entitled to declaratory or injunctive relief to
22 enjoin the unlawful conduct alleged herein; and
- 23 h. Whether Plaintiffs and Class members have sustained damages as a result of Padlet's
24 conduct and, if so, what is the appropriate measure of damages or restitution.

25 180. **Superiority:** A class action is superior to all other available methods for the fair and
26 efficient adjudication of this controversy since joinder of all members is impracticable. This
27 proposed class action presents fewer management difficulties than individual litigation and
28

1 provides the benefits of a single adjudication, economies of scale and comprehensive supervision
2 by a single, able court. Furthermore, as the damages individual Class members have suffered may
3 be relatively small, the expense and burden of individual litigation make it impossible for Class
4 members to individually redress the wrongs done to them. There will be no difficulty in
5 management of this action as a class action.

6 181. Plaintiffs reserve the right to revise the foregoing class allegations and definitions
7 based on facts learned and legal developments following additional investigation, discovery, or
8 otherwise.

9 VI. TOLLING OF THE STATUTE OF LIMITATIONS

10 182. Any applicable statute(s) of limitations have been tolled by Padlet's and its
11 affiliates' knowing and active concealment and denial of the facts alleged herein. Plaintiffs and
12 Class members could not have reasonably discovered the true nature of Padlet's data-harvesting
13 scheme because Padlet purposely concealed it. Plaintiffs' claims were thus tolled under the
14 discovery rule.

15 183. The causes of action alleged herein did not accrue until Plaintiffs and Class members
16 discovered or could have discovered Padlet's data-harvesting scheme.

17 184. As alleged above, Plaintiffs and Class members had no way of knowing about
18 Padlet's data-harvesting scheme. Padlet concealed the scheme while simultaneously claiming that
19 it protects PI and students' privacy.

20 185. To this day, Padlet fails to disclose the full extent of, and risks associated with, its
21 data-harvesting scheme.

22 186. Within any applicable statutes of limitation, Plaintiffs and Class members could not
23 have discovered, through the exercise of reasonable diligence, that Padlet was concealing the
24 conduct complained of herein and misrepresenting the nature of its business.

25 187. Plaintiffs and Class members did not know facts that would have caused a
26 reasonable person to suspect that there was a data-harvesting scheme that would result in a private
27 corporation collecting, manipulating, and monetizing every aspect of their children's lives and their
28

own interactions with their children's schools and school districts. Padlet also withheld any and all information that would give a reasonable person knowledge of the data-harvesting scheme and disclaimed that it unlawfully monetized data about and belonging to Plaintiffs and Class members.

188. For ordinary consumers, the existence of the data-harvesting scheme is still unknown. For these reasons, all applicable statutes of limitation have been tolled by operation of the discovery rule with respect to the claims in this litigation.

VII. CAUSES OF ACTION

COUNT I: Violation of the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*

(On behalf of Plaintiffs and the Nationwide Class)

189. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though fully set forth herein.

190. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

191. The Federal Wiretap Act protects both the sending and receipt of communications.

192. 18 United States Code section 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

193. Padlet's actions in intercepting and tracking user communications were intentional. Upon information and belief, Padlet is aware that it is intercepting communications and has taken no remedial actions.

194. Padlet's interception of internet communications that Plaintiffs and Nationwide Class members were sending and receiving was done contemporaneously with Plaintiffs' and Nationwide Class members' sending and receipt of those communications.

195. The communications intercepted by Padlet included "contents" of electronic communications made from Plaintiffs and Nationwide Class members to websites and other web properties other than Padlet's in the form of detailed URL requests, webpage browsing histories, search queries, and other information that Plaintiffs and Nationwide Class members sent to those

1 websites and for which Plaintiffs received communications in return from those websites.

2 196. These transmissions were tracked and intercepted without authorization and are
3 “transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in
4 whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that
5 affects interstate commerce[,]” and were therefore “electronic communications” within the
6 meaning of 18 United States Code section 2510(12).

7 197. The following constitute “devices” within the meaning of 18 United States Code
8 section 2510(5):

- 9 a. The computer codes and programs that Padlet used to track Plaintiffs’ and Nationwide
10 Class members’ communications;
11 b. Plaintiffs’ and Nationwide Class members’ browsers and mobile applications;
12 c. Plaintiffs’ and Nationwide Class members’ computing and mobile devices;
13 d. Padlet’s servers; and
14 e. The plan that Padlet carried out to effectuate its tracking and interception of Plaintiffs’
15 and Nationwide Class members’ communications.

16 198. Padlet, in its conduct alleged here, was not providing an “electronic communication
17 service” as that term is defined in 18 United States Code section 2510(12) and used elsewhere in
18 the Federal Wiretap Act. Padlet was not acting as an Internet Service Provider.

19 199. Padlet was not an authorized party to the communications because Plaintiffs and
20 Nationwide Class members were unaware of Padlet’s interceptions and did not knowingly send any
21 communications to Padlet when Padlet intercepted the communications between Plaintiffs and web
22 properties other than Padlet’s. Padlet could not manufacture its own status as a party to Plaintiffs’
23 and Nationwide Class members’ communications with others by surreptitiously redirecting or
24 intercepting those communications.

25 200. Plaintiffs and Nationwide Class members did not consent to Padlet’s continued
26 gathering of their communications.

27 201. After intercepting the communications, Padlet simultaneously disclosed the contents
28

1 of the communications to over 160 unauthorized third parties, including, among many others, to
 2 LiveRamp, Nielsen, TransUnion, PulsePoint, Epsilon, Google, and Meta, knowing or having
 3 reason to know that such information was obtained through the interception of electronic
 4 communications in violation of 18 United States Code section 2511(1)(a).

5 202. Padlet disclosed the contents of those communications to third parties for the
 6 purpose of committing a crime or tort, including but not limited to, the tort of intrusion upon
 7 seclusion.

8 203. After intercepting the communications, Padlet then used the contents of the
 9 communications knowing or having reason to know that such information was obtained through
 10 the interception of electronic communications in violation of 18 United States Code section
 11 2511(1)(a).

12 204. As a result of this conduct, the Court may assess statutory damages to Plaintiffs and
 13 Nationwide Class members; injunctive and declaratory relief; punitive damages in an amount to be
 14 determined by a jury, but sufficient to prevent the same or similar conduct by Padlet in the future,
 15 and reasonable attorneys' fees and other litigations costs reasonably incurred.

16 **COUNT II: Violation of the California Invasion of Privacy Act ("CIPA")**

17 **Cal. Penal Code § 631**

18 *(On behalf of Plaintiffs and the Nationwide Class)*

19 205. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though
 20 fully set forth herein.

21
 22 206. CIPA is codified at California Penal Code sections 630 through 638.55. The
 23 Legislature declared its purpose in section 630:

24 The Legislature hereby declares that advances in science and technology
 25 have led to the development of new devices and techniques for the purpose
 26 of eavesdropping upon private communications and that the invasion of
 27 privacy resulting from the continual and increasing use of such devices and
 28 techniques has created a serious threat to the free exercise of personal
 liberties and cannot be tolerated in a free and civilized society.

1 207. The Legislature thus directed that CIPA’s protections extend across the developing
 2 field of technology, and that the Act reach “new devices and techniques” as they emerge. Cal. Penal
 3 Code § 630. California Penal Code section 631(a) provides, in pertinent part:

4 Any person who, by means of any machine, instrument, or contrivance, or
 5 in any other manner . . . willfully and without the consent of all parties to the
 6 communication, or in any unauthorized manner, reads, or attempts to read,
 7 or to learn the contents or meaning of any message, report, or communication
 8 while the same is in transit or passing over any wire, line, or cable, or is
 9 being sent from, or received at any place within this state; or who uses, or
 10 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, is
 punishable by a fine not exceeding two thousand five hundred dollars[.]

11 208. Section 631(a) creates liability in four distinct circumstances: (i) intentionally
 12 tapping or making an unauthorized connection with a telegraph or telephone wire, line, cable, or
 13 instrument; (ii) willfully and without the consent of all parties reading, attempting to read, or
 14 learning the contents or meaning of a communication while it is in transit; (iii) using or attempting
 15 to use information so obtained; and (iv) aiding, agreeing with, employing, or conspiring with any
 16 person to do any of the foregoing.

17 209. Plaintiffs bring this Count under the second, third, and fourth bases for liability.
 18 Plaintiffs do not assert a claim under the first basis.

19 **A. Padlet acted willfully and without the consent of any party.**

20 210. Neither Plaintiffs, nor Class members, nor their parents consented to Padlet’s
 21 reading, learning, use, or disclosure of their communications. As alleged above, Padlet never sought
 22 consent from any student or parent; school personnel created Plaintiffs’ accounts; Plaintiffs and
 23 their parents were never presented with Padlet’s terms or policies; and no school official had
 24 authority to consent on a parent’s behalf.

25 211. Padlet’s conduct was willful and intentional. Padlet designed, built, configured, and
 26 deployed the code that effects the conduct alleged in this Count, selected each third-party recipient,
 27 determined what data each would receive, and maintained those configurations over time.
 28

B. Padlet acted by means of machines, instruments, and contrivances.

212. Each of the following constitutes a “machine, instrument, or contrivance” within the meaning of section 631(a), and, in the alternative, Padlet’s deliberate and purposeful scheme falls within the statute’s catch-all, “or in any other manner”:

- a. the tracking code, software development kits, tags, and pixels Padlet wrote into and embedded within the Padlet Platform;
- b. the third-party pixels Padlet caused to be returned to and executed on Plaintiffs’ browsers, including those of Meta Platforms and Integral Ad Science;
- c. Padlet’s servers and the software running on them; and
- d. the browsers and devices on which Plaintiffs accessed the Padlet Platform.

C. The conduct occurred contemporaneously, while the communications were in transit.

213. Padlet’s tracking code executes in the student’s browser at the moment the student acts. When a student types text, clicks a link, enters a search term, submits a post, uploads a file, or makes an audio or video recording, that code captures the communication and transmits it to third parties in the same instant.

214. These transmissions occur simultaneously with the students’ communications and independent of any storage of those communications by Padlet. Padlet does not receive a communication, store it, and later transmit it. The capture and the transmission are contemporaneous with the communication itself.

215. Forensic testing captured these transmissions occurring in real time. Accordingly, the conduct alleged in this Count occurred while Plaintiffs’ communications were in transit or passing over a wire, line, or cable, and while those communications were being sent from and received at places within the State of California.

D. Padlet read and learned the contents of communications to which it was not a party, and used the information so obtained.

1 216. The Padlet Platform provides built-in links to, and embeds content from, third-party
2 properties outside Padlet, including internet search, YouTube, Spotify, and other online databases
3 and websites.

4 217. When Plaintiffs and Class members used those functions, they sent communications
5 to those third-party properties, including search queries, detailed URL requests, and the contents of
6 their requests, and received communications in return.

7 218. Padlet was not a party to those communications. Padlet nonetheless read, attempted
8 to read, and learned the contents and meaning of those communications while they were in transit,
9 including Plaintiffs' search terms, the links they clicked, and their browsing activity.

10 219. Padlet then used the contents of those communications, and information so obtained,
11 in numerous ways (including to develop, improve, and market the Padlet Platform, and to transmit
12 that content to the third parties identified in this Complaint) in violation of section 631(a)'s third
13 basis for liability.

14 **E. Padlet aided, employed, and conspired with third parties to intercept**
15 **Plaintiffs' communications.**

16 220. Padlet is a party to communications between students and the Padlet Platform itself.
17 The third parties identified in this Complaint are not parties to those communications.

18 221. Padlet embedded within the Padlet Platform the code of more than 160 third parties.
19 That code caused Plaintiffs' communications — including the content students created, the pages
20 they viewed, the time they spent, their search terms, and their persistent unique identifiers — to be
21 transmitted to those third parties in a duplicate, real-time stream, simultaneously with the students'
22 communications with Padlet.

23 222. Those third parties did not act as mere tools, conduits, or recording devices operated
24 for Padlet's benefit. They are independent businesses — including more than forty data brokers
25 and thirteen identity-resolution companies — that maintain their own commercial datasets, receive
26 data from thousands of unrelated sources, and use the data they receive for their own purposes and
27 for the purposes of their own paying customers. By way of example:
28

- a. LiveRamp, Nielsen, TransUnion, and Epsilon operate identity-resolution businesses whose function is to attach data received from one source to preexisting profiles assembled from other sources, and to resell the resulting profiles to their own customers;
- b. the persistent identifiers Padlet transmitted, including UUIDs and Google advertising identifiers, are linkage keys that permit these companies to recognize the same child across sessions, across devices, and across unrelated websites, and to index that child's Padlet classroom activity against activity occurring entirely outside the Padlet Platform;
- c. Meta Platforms and Integral Ad Science returned tracking pixels that executed on Plaintiffs' browsers and transmitted Plaintiffs' data directly to those companies; and
- d. Google used its advertising identifiers and pixel-matching technology to integrate Plaintiffs' classroom activity into Google's broader cross-site advertising and analytics ecosystem.

223. Each of these uses is independent of, and unnecessary to, any service those companies provide to Padlet. Padlet does not receive, and cannot use, the cross-site and cross-device profiles those companies construct from the data Padlet sends them. The profiles are built for the recipients' own commercial benefit.

224. Padlet knew of and intended these transmissions. Padlet selected each third party, embedded or permitted the embedding of its code, configured the categories of data transmitted to it, and maintained those configurations over the period alleged.

225. By this conduct, Padlet aided, agreed with, employed, and conspired with those third parties to read and learn the contents and meaning of Plaintiffs' and Class members' communications while in transit, and to use the information so obtained, without the consent of all parties.

F. Injury and relief.

226. Plaintiffs and Class members have been injured by Padlet's violations of section 631(a), including through the loss of their right to control the dissemination and use of their communications, the loss of privacy, and the diminution in value of their personal information.

227. Pursuant to California Penal Code section 637.2(a), Plaintiffs and Class members seek the greater of \$5,000 per violation or three times the amount of actual damages sustained. Each transmission of a Plaintiff's or Class member's communication to each third-party recipient constitutes a separate violation.

228. It is not a necessary prerequisite to this action that Plaintiffs or Class members have suffered, or be threatened with, actual damages. Cal. Penal Code § 637.2(c).

229. Plaintiffs and Class members further seek to enjoin and restrain Padlet's continuing violations pursuant to California Penal Code section 637.2(b).

COUNT III: Violation of the California Invasion of Privacy Act ("CIPA")

Cal. Penal Code § 632

(On behalf of Plaintiffs and the Nationwide Class)

230. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though fully set forth herein.

231. California Penal Code section 632(a) provides, in pertinent part:

A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars[.]

232. A "confidential communication" is "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto." Cal. Penal Code § 632(c). A communication is confidential where a party "has an objectively reasonable expectation that the conversation is not being overheard or recorded."

233. Section 632 contains no party exception. Unlike section 631(a), section 632 reaches every person who uses a recording device to record a confidential communication without the consent of all parties, including a person who is itself a party to that communication. Padlet is

1 therefore directly liable under section 632 for its own recording of Plaintiffs' and Class members'
2 communications.

3 **A. Padlet intentionally used electronic recording devices.**

4 234. Section 632 does not define "device." Consistent with the Legislature's express
5 direction that CIPA extend across the developing field of technology, Cal. Penal Code § 630,
6 software constitutes a device within the meaning of section 632(a).

7 235. Each of the following is an electronic amplifying or recording device within the
8 meaning of section 632(a):

- 9 a. the tracking, logging, and event-capture code Padlet wrote into and deployed within the
10 Padlet Platform;
- 11 b. the software development kits, tags, and pixels Padlet embedded in the Padlet Platform;
- 12 c. the third-party pixels Padlet caused to be returned to and executed on Plaintiffs'
13 browsers, including those of Meta Platforms and Integral Ad Science; and
- 14 d. the servers and software Padlet used to receive, record, retain, and transmit the captured
15 communications.

16 236. Padlet used those devices intentionally. It designed, configured, and deployed them
17 for the specific purpose of capturing and recording what students wrote, said, submitted, and
18 searched for on the Padlet Platform, and it did so knowingly and for its own commercial benefit.

19 **B. Padlet recorded the contents of communications, not merely behavioral data.**

20 237. Padlet recorded the contents of Plaintiffs' and Class members' communications,
21 including:

- 22 a. the text, images, files, and other content students composed and posted to Padlet Boards
23 and Sandboxes;
- 24 b. the comments and messages students directed to their teachers and to other students;
- 25 c. audio recordings of students' voices and video recordings of students' faces and
26 surroundings, made using the camera, video recorder, and audio recorder built into the
27 Padlet Platform;

- d. the search terms students entered while using the Padlet Platform and the built-in links it provides; and
- e. the lessons, assignments, responses, and assessments students completed and submitted through the Platform.

238. Each of these is a communication. Each conveys the substance, purport, and meaning of what a student wrote, said, recorded, asked, or submitted, and each reflects the student's own thoughts, ideas, and expression. None is mere behavioral or navigational metadata.

C. The communications were confidential.

239. Plaintiffs and Class members had an objectively reasonable expectation that their communications on the Padlet Platform were not being overheard or recorded by anyone other than their teachers and their classmates.

240. That expectation was objectively reasonable for reasons specific to this setting and absent from ordinary consumer internet browsing:

- a. Plaintiffs and Class members are children, and many, including M.C. 2, are under the age of 13.
- b. The communications occurred within a compulsory educational environment. Plaintiffs did not select the Padlet Platform, could not decline to use it without jeopardizing their education, and were never presented with any terms, policy, or disclosure describing Padlet's data practices.
- c. The Padlet Platform is provisioned by the school and presented as a closed classroom space. Boards and Sandboxes are created by school personnel for a defined class, and the audience for a student's post is that class. A student posting to a class Board reasonably understands the audience to be the teacher and the enrolled students, and no one else.
- d. The communications include audio and video recordings of children — their voices, their faces, their classrooms, and their homes.

- 1 e. The communications are singled out for protection by federal law. COPPA restricts the
2 collection, use, and disclosure of the personal information of children under 13 absent
3 verifiable parental consent, and FERPA restricts the disclosure of student education
4 records. Communications that Congress has specifically protected are not
5 communications a child may be expected to assume are being recorded and monetized.
- 6 f. Padlet represented to students, parents, and schools that the Padlet Platform is “private”
7 and “secure,” that student “data is never monetized or shared for advertising purposes,”
8 and that Padlet “ha[s] not shared [students’] PI with any third party for direct marketing
9 purposes.” A party’s expectation that a communication is not being recorded is
10 objectively reasonable where the operator of the service has represented that it is not.

11 241. Nothing about these communications resembles the open, public-facing internet
12 activity that has been held non-confidential. Plaintiffs were not shopping, browsing a public
13 commercial website, or transacting with a merchant. They were performing compelled schoolwork
14 inside a classroom application their school required them to use, in a space Padlet held out as
15 private.

16 **D. Padlet acted without the consent of all parties.**

17 242. Padlet did not obtain the consent of all parties to the confidential communications it
18 recorded. Neither Plaintiffs, nor Class members, nor their parents consented to the recording.
19 School personnel created Plaintiffs’ accounts, and no school official had authority to consent to the
20 recording of a child’s confidential communications on the child’s or the parent’s behalf.

21 **E. Injury and relief.**

22 243. Plaintiffs and Class members have been injured by Padlet’s violations of section
23 632, including through the loss of privacy, the loss of their right to control the dissemination and
24 use of their communications, and the diminution in value of their personal information.

25 244. Pursuant to California Penal Code section 637.2(a), Plaintiffs and Class members
26 seek the greater of \$5,000 per violation or three times the amount of actual damages sustained.
27 Each confidential communication recorded by Padlet constitutes a separate violation.
28

245. It is not a necessary prerequisite to this action that Plaintiffs or Class members have suffered, or be threatened with, actual damages. Cal. Penal Code § 637.2(c).

246. Plaintiffs and Class members further seek to enjoin and restrain Padlet's continuing violations pursuant to California Penal Code section 637.2(b).

COUNT IV: Violation of the Comprehensive Computer Data Access and Fraud Act
(“CDAFA”), Cal. Penal Code § 502 *et seq.*

(On behalf of Plaintiffs and the Nationwide Class)

247. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though fully set forth herein.

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

249. Plaintiffs’ and the Nationwide Class members’ devices on which they accessed Padlet’s services, including computers, smart phones, and tablets, constitute computers or “computer systems” within the meaning of CDAFA. *Id.* § 502(b)(5).

250. As described herein, Padlet accessed, took, copied, analyzed, used—and actively facilitated, aided, and assisted more than one-hundred third-party companies in accessing, taking, copying, analyzing, and using—Plaintiffs and the Nationwide Class members’ data. Plaintiffs and the Nationwide Class members are the owners of that data and bring this claim as owners of that data within the meaning of Cal. Penal Code section 502(e)(1).

251. Padlet violated Cal. Penal Code section 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' and the Nationwide Class members' data as described herein.

252. Padlet also violated Cal. Penal Code sections 502(c)(6) and 502(c)(7) by knowingly and without permission providing or assisting in providing a means of accessing Plaintiffs' and Nationwide Class members' computer systems by a multitude of third-party companies and in

1 knowingly and without permission causing Plaintiffs' and Nationwide Class members' computer
2 systems to be accessed by those third-party companies.

3 253. Padlet was unjustly enriched by acquiring the valuable PI of Plaintiffs and the
4 Nationwide Class members without permission and using and sharing it for Padlet's own financial
5 benefit to advance its business interests.

6 254. Plaintiffs and the Nationwide Class members retain a stake in the profits that Padlet
7 earned from the misuse of their activity and personally identifiable information because, under the
8 circumstances, it is unjust for Padlet to retain those profits.

9 255. Padlet accessed, copied, took, analyzed, and used data from Plaintiffs' and the
10 Nationwide Class members' computer systems, and actively facilitated, aided, and assisted third-
11 party companies in accessing, copying, taking, analyzing, and using data from Plaintiffs' and the
12 Nationwide Class members' computer systems, in and from the State of California, where Padlet
13 marketed and sold its products. Accordingly, Padlet caused the access of their computers in
14 California and is therefore deemed to have accessed and facilitated access to their computer systems
15 in California.

16 256. As a direct and proximate result of Padlet's unlawful conduct within the meaning of
17 Cal. Penal Code section 502, Padlet has caused loss to Plaintiffs and the Nationwide Class members
18 and has been unjustly enriched in an amount to be proven at trial.

19 257. Plaintiffs and the Nationwide Class members seek compensatory damages and/or
20 disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable
21 relief.

22 258. Plaintiffs and the Nationwide Class members are entitled to punitive or exemplary
23 damages pursuant to Cal. Penal Code section 502(e)(4) because Padlet's violations were willful
24 and, upon information and belief, Padlet is guilty of oppression or malice as defined by Cal. Civil
25 Code section 3294.

26 259. Plaintiffs and the Nationwide Class members are also entitled to recover their
27 reasonable attorneys' fees pursuant to Cal. Penal Code section 502(e).
28

COUNT V: Violation of California’s Unfair Competition Law (“UCL”),

Cal. Bus. & Prof. Code § 17200, *et seq.*

(On behalf of Plaintiffs and the Nationwide Class)

260. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though fully set forth herein.

261. Plaintiffs lack an adequate remedy at law.

262. In addition or as an alternative to legal remedies sought herein, Plaintiffs seek equitable relief to the extent that legal remedies are inadequate.

263. The UCL prohibits any “unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising.” Cal. Bus. & Prof. Code § 17200. By engaging in the aforementioned practices, Padlet has violated the UCL.

264. A plaintiff may pursue a claim under the UCL through any or all of three prongs: the unlawful prong, the unfair prong, or the fraudulent prong.

265. Padlet’s conduct violated the spirit and letter of the laws as alleged herein, which protect property, economic, and privacy interests and prohibit unauthorized disclosure and collection of private communications and PI.

266. Padlet’s unfair acts and practices include its violation of property, economic, and privacy interests of children protected by federal and state laws.

267. To establish liability under the “unfair” prong, Plaintiffs and the Nationwide Class members need not establish that these statutes were actually violated, although the allegations herein establish that they were. The foregoing allegations are tethered to underlying constitutional, statutory, or regulatory provisions; describe practices that are immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers; and show that the negative impact of Padlet’s practices on school-aged children and their parents far outweighs the reasons, justifications, and motives of Padlet.

268. The foregoing allegations also establish liability under the “unlawful” prong, as they show that Padlet violated an array of state and federal laws protecting individual privacy and

1 property.

2 269. Plaintiffs and the Nationwide Class members have suffered injury-in-fact, including
3 the loss of money or property, as a result of Padlet's unfair and unlawful practices, which include
4 the unauthorized disclosure and taking of their PI that has value as demonstrated by its use and
5 disclosure by Padlet. Plaintiffs and the Nationwide Class members have suffered harm in the form
6 of diminution of the value of their private and personally identifiable data and content.

7 270. Padlet's actions caused damage to and loss of Plaintiffs' and the Nationwide Class
8 members' property right to control the dissemination and use of their PI and communications.

9 271. Padlet's actions also prevented the development of a legitimate market for PI in
10 which Plaintiffs could fairly choose to participate. And Plaintiffs would consider participating in a
11 market for their information if their participation was voluntary; the terms of the transaction were
12 transparent; they controlled what information was taken and how it could be used; and they were
13 fairly compensated by those benefiting from their information.

14 272. Because Padlet and other education-technology companies simply take valuable PI
15 without effective consent and monetize it as they see fit, (1) no lawful market for that data exists
16 and (2) even if it did, Padlet's unlawful taking and use of that data has diminished the value of that
17 data.

18 273. Padlet reaped unjust profits and revenues in violation of the UCL. This includes
19 Padlet's profits and revenues from its sale and licensing of its products, which Padlet develops,
20 delivers, maintains, and improves using the PI of Plaintiffs and the Nationwide Class members, as
21 well as through its data sharing with innumerable third parties. Plaintiffs and the Nationwide Class
22 members seek restitution and disgorgement of these unjust profits and revenues.

23 **COUNT VI: Invasion of Privacy—Intrusion Upon Seclusion**

24 ***(On behalf of Plaintiffs and the Nationwide Class)***

25 274. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though
26 fully set forth herein.

27 275. Under California law, Plaintiffs asserting claims for intrusion upon seclusion must
28

1 plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to
2 a reasonable person.

3 276. Padlet intentionally intruded into Plaintiffs’ and Nationwide Class members’ private
4 affairs in a highly offensive manner through its systematic and pervasive collection, accessing,
5 downloading, transferring, storing, use, and sharing of Plaintiffs’ and Nationwide Class members’
6 PI.

7 277. Plaintiffs and Nationwide Class members maintained a reasonable expectation of
8 privacy interest in their PI absent consent to tracking, collection, and disclosure practices. Plaintiffs
9 and Nationwide Class members never consented—and in the case of Padlet school-licensed
10 products, never even had the opportunity to consent—to Padlet’s data practices.

11 278. The reasonableness of this expectation of privacy is reflected in COPPA, which
12 prevents the collection, use, and sharing of personal information of children under 13 by private
13 companies without parental consent, and FERPA, which requires schools to obtain parental consent
14 before sharing students’ personal information with even legitimate “school officials,” which Padlet
15 is not.

16 279. The reasonableness of this expectation of privacy is also reflected in longstanding
17 custom and practice; security measures intended to prevent unauthorized access to PI, especially
18 concerning young children; state, federal, and international laws protecting a right to financial
19 privacy; and the privacy policies and other assurances of protection by applications that use Padlet
20 discussed herein, among other indicia.

21 280. Plaintiffs and Nationwide Class members could not reasonably expect that, by
22 simply participating in their education and completing required activities, Padlet would collect,
23 store, manipulate, monetize, and share such voluminous and far-reaching categories of PI; prevent
24 Plaintiffs and Nationwide Class members from reviewing, correcting, or controlling that
25 information; and use that information in ways that were harmful to Plaintiffs and Nationwide Class
26 members.

27 281. Individuals also maintain a reasonable expectation of privacy when they are using
28

1 products in a compulsory environment such as public schools. Padlet's collection of Plaintiffs' and
2 Nationwide Class members' information while logged into the Padlet Platform was unreasonable.

3 282. COPPA demonstrates that students under the age of 13 have a reasonable
4 expectation of privacy in their personal information while using online services in schools, and
5 Padlet's collection, use, and disclosure of Plaintiffs' personal information without providing notice
6 to Plaintiffs' parents and without obtaining verifiable parental consent in violation of COPPA is
7 highly offensive to a reasonable person.

8 283. FERPA demonstrates that students have a reasonable expectation of privacy in their
9 education records, and Padlet's disclosure of those records to third parties without the knowledge
10 or consent of the students' parents—causing schools to violate FERPA—renders its conduct highly
11 offensive to a reasonable person.

12 284. Padlet's intrusions upon Plaintiffs' and Nationwide Class members' private affairs
13 and concerns are highly offensive to a reasonable person, especially considering (a) the highly
14 sensitive and personal nature of Plaintiffs' and Nationwide Class members' PI; (b) the extensive
15 scope of PI obtained by Padlet, including years of historical data; (c) Padlet's intent to profit from
16 Plaintiffs' and Nationwide Class members' PI by selling it outright (e.g., back to schools, its
17 "customers," and myriad other third parties) and using it to develop and market its products and
18 services; (d) Padlet's use of subterfuge to intrude into Plaintiffs' and Nationwide Class members'
19 electronic devices for the purpose of collecting their PI; (e) the surreptitious and unseen nature of
20 Padlet's data collection with respect to consumers, (f) Padlet's disclosure of the PI to more than
21 160 unauthorized third parties, many of which are data brokers and other AdTech companies that
22 sell or use the data for targeted advertising purposes and for their own commercial benefit, and (g)
23 Padlet's failure to obtain valid consent.

24 285. Padlet's conduct would be highly offensive to a reasonable person, particularly
25 given Padlet's extensive and false public statements regarding its commitment to user privacy and
26 given that Padlet designs products to be used by children, including young children. The manner
27 of the invasion—collection through students' use of education tools in a compulsory setting—is
28

1 also highly offensive.

2 286. Padlet's invasions of privacy caused Plaintiffs and Nationwide Class members the
3 following damages:

4 a. Nominal damages;

5 b. The diminution in value of Plaintiffs' and Nationwide Class members' private
6 information;

7 c. The loss of privacy due to Padlet rendering no longer private the confidential and
8 personal information that Plaintiffs and Nationwide Class members intended to remain
9 private; and

10 d. The fair value of Plaintiffs' and Nationwide Class members' PI and data. Padlet took
11 something of value from Plaintiffs and Nationwide Class members—their PI and data—
12 and derived benefits therefrom without Plaintiffs' and Nationwide Class members'
13 knowledge or consent and without Padlet sharing the fair benefit of such value with
14 them.

15 287. Padlet invaded Plaintiffs' and Nationwide Class members' privacy with oppression,
16 fraud, or malice.

17 288. As a result of Padlet's invasions of privacy, Plaintiffs and Nationwide Class
18 members seek actual damages, compensatory damages, restitution, disgorgement, general
19 damages, nominal damages, unjust enrichment, punitive damages, and any other relief the Court
20 deems just.

21 **COUNT VII: Maryland Wiretapping and Electronic Surveillance Act,**

22 **Md. Code Ann., Cts. & Jud. Proc. §§ 10-401, *et seq.***

23 ***(On Behalf of Plaintiffs and the Maryland Subclass)***

24 289. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though
25 fully set forth herein.

26 290. Plaintiffs bring this claim individually and on behalf of the Maryland Subclass.

27 291. The Maryland Wiretapping and Electronic Surveillance Act ("Maryland Wiretap
28

1 Act”), Md. Code Ann., Cts. & Jud. Proc. §§ 10-401, *et seq.*, prohibits the interception of any wire,
2 oral, or electronic communications without the consent of all of the parties to the communication.

3 292. The Act confers a civil cause of action on “any person whose wire, oral, or electronic
4 communication is intercepted, disclosed, or used in violation of this subtitle.” Md. Code Ann., Cts.
5 & Jud. Proc. § 10-410(a).

6 293. The Maryland Wiretap Act provides that it is unlawful for any person to “willfully
7 intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept,
8 any wire, oral, or electronic communication,” or “willfully disclose, or endeavor to disclose, to any
9 other person the contents of any wire, oral, or electronic communication, knowing or having reason
10 to know that the information was obtained through the interception of a wire, oral, or electronic
11 communication in violation of this subtitle,” or “willfully use, or endeavor to use, the contents of
12 any wire, oral, or electronic communication, knowing or having reason to know that the information
13 was obtained through the interception of a wire, oral, or electronic communication in violation of
14 this subtitle.” Md. Code Ann., Cts. & Jud. Proc. § 10-402(a)(1)-(3).

15 294. In addition, “a person or entity providing an electronic communication service to
16 the public may not intentionally divulge the contents of any communication . . . while in
17 transmission on that service to any person or entity other than an addressee or intended recipient of
18 the communication or an agent of the addressee or intended recipient.” Md. Code Ann., Cts. & Jud.
19 Proc. § 10-402(d)(1).

20 295. “Intercept” means “the aural or other acquisition of the contents of any wire,
21 electronic, or oral communication through the use of any electronic, mechanical, or other device.”
22 Md. Code Ann., Cts. & Jud. Proc. § 10-401(10).

23 296. “Electronic communication” means “any transfer of signs, signals, writing, images,
24 sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,
25 electromagnetic, photoelectronic, or photooptical system.” Md. Code Ann., Cts. & Jud. Proc. § 10-
26 401(5)(i).

27 297. “Contents” includes “any information concerning the identity of the parties to the
28

1 communication or the existence, substance, purport, or meaning of that communication.” Md. Code
2 Ann., Cts. & Jud. Proc. § 10-401(4).

3 298. An “electronic communication service” means “any service that provides to users
4 of the service the ability to send or receive wire or electronic communications.” Md. Code Ann.,
5 Cts. & Jud. Proc. § 10-401(6).

6 299. The Padlet Platform is an “electronic communication service” within the meaning
7 of Md. Code Ann., Cts. & Jud. Proc. § 10-401(6).

8 300. Plaintiffs’ and the Maryland Subclass members’ communications with the Padlet
9 Platform are electronic communications under the Maryland Wiretap Act.

10 301. Padlet’s actions in intercepting and tracking user electronic communications were
11 intentional. Upon information and belief, Padlet is aware that it is intercepting electronic
12 communications and has taken no remedial actions.

13 302. Padlet’s interception of electronic communications that Plaintiffs and Maryland
14 Subclass members were sending and receiving was done contemporaneously with Plaintiffs’ and
15 Maryland Subclass members’ sending and receipt of those communications.

16 303. The communications intercepted by Padlet included “contents” of electronic
17 communications made from Plaintiffs and Maryland Subclass members to websites and other web
18 properties other than Padlet’s in the form of chats with other students and comments on teachers’
19 and other students’ digital boards and whiteboards.

20 304. Those contents also included detailed URL requests, webpage browsing histories,
21 search queries, and other information that Plaintiffs and Maryland Subclass members sent to those
22 websites and for which Plaintiffs received communications in return from those websites.

23 305. Padlet was not an authorized party to the communications because Plaintiffs and
24 Maryland Subclass members were unaware of Padlet’s interceptions and did not knowingly send
25 any electronic communications to Padlet when Padlet intercepted the electronic communications
26 between Plaintiffs and web properties other than Padlet’s. Padlet could not manufacture its own
27 status as a party to Plaintiffs’ and Maryland Subclass members’ communications with others by
28

1 surreptitiously redirecting or intercepting those communications.

2 306. Plaintiffs and Maryland Subclass members did not consent to Padlet's continued
3 gathering of their electronic communications.

4 307. After intercepting the electronic communications, Padlet simultaneously disclosed
5 the contents of the communications to unauthorized third parties, including but not limited to
6 LiveRamp, TransUnion, PulsePoint, Epsilon, Google, and Meta, knowing or having reason to know
7 that such information was obtained through the interception of electronic communications in
8 violation of the Maryland Wiretap Act.

9 308. Padlet disclosed the contents of those communications with third parties for the
10 purpose of committing a crime or tort, including but not limited to, the tort of intrusion upon
11 seclusion.

12 309. After intercepting the communications, Padlet then used the contents of the
13 communications knowing or having reason to know that such information was obtained through
14 the interception of electronic communications in violation of Md. Code Ann., Cts. & Jud. Proc. §
15 10-402(a).

16 310. Padlet's actions were at all relevant times knowing, willful, and intentional.

17 311. Pursuant to Md. Code Ann., Cts. & Jud. Proc. § 10-410(a), Plaintiffs and the
18 Maryland Subclass members have been damaged by the interception, disclosure, and/or use of their
19 communications in violation of the Maryland Wiretap Act and are entitled to: (1) damages, in an
20 amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages
21 suffered by Plaintiffs and the Maryland Subclass members, or (b) liquidated damages of whichever
22 is the greater of \$100 per day per violation or \$1,000; (2) punitive damages; and (3) reasonable
23 attorneys' fees and other litigation costs reasonably incurred.

24 **COUNT VIII: Quasi Contract (Unjust Enrichment)**

25 ***(On Behalf of Plaintiffs and the Nationwide Class Pursuant to California Law)***

26 312. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though
27 fully set forth herein.
28

1 313. Plaintiffs lack an adequate remedy at law.

2 314. In addition or as an alternative to legal remedies sought herein, Plaintiffs seek
3 equitable relief to the extent that legal remedies are inadequate.

4 315. Plaintiffs conferred a benefit upon Padlet, namely, provision of their PI to Padlet
5 through their compelled use of the Padlet Platform at school.

6 316. This benefit was not conveyed gratuitously. Plaintiffs are required to go to school
7 and were required to use the Padlet Platform in connection with their education, and they did not
8 use the Platform with the intention of providing their PI to Padlet or any third party.

9 317. Padlet appreciated the fact that it obtained this benefit from Plaintiffs, namely, it
10 understands that PI is the raw material that fuels its business, without which Padlet would have no
11 product and no business.

12 318. It would be inequitable for Padlet to retain that benefit without payment to Plaintiffs
13 of the value that benefit has conferred to Padlet.

14 319. More specifically, Padlet acquired and compromised troves of PI that rightfully
15 belong to Plaintiffs and Nationwide Class members without effective consent through intentionally
16 deceptive practices conducted in connection with students' compulsory use of the Padlet Platform.

17 320. Padlet obtained access to this information only by marketing and selling its Platform
18 for use by children in the compulsory environment of K–12 education.

19 321. Padlet has built, developed, improved, marketed, and delivered an ever-growing
20 suite of products using the PI of Plaintiffs and Nationwide class members. It has further derived
21 profits and other tangible and intangible benefits from its improper collection, use, and disclosure
22 of Plaintiffs' and Nationwide Class members' data.

23 322. But for collecting children's PI without effective consent, Padlet could not have
24 grown its business, acquired numerous other tangible and intangible assets, developed other
25 applications, and received millions of dollars in investment capital to achieve a multimillion-dollar
26 valuation.

27 323. Padlet has also directly and substantially profited from its use, storage, aggregation,
28

1 and disclosure of Plaintiffs' and Nationwide Class members' data. Indeed, Plaintiffs' and
2 Nationwide Class members' data powers Padlet's ever-growing ecosystem of products and
3 services. Without Plaintiffs' and Nationwide Class members' PI unlawfully taken by Padlet, Padlet
4 would cease to operate in its current form.

5 324. In exchange for these benefits to Padlet, Plaintiffs and Nationwide Class members
6 received nothing but educational services to which they were already legally entitled and required
7 to receive.

8 325. To benefit its bottom line, Padlet deprived Plaintiffs and Nationwide Class members
9 of their property, security, privacy, and autonomy.

10 326. Padlet harmed Plaintiffs and Nationwide Class members by, among other harms,
11 subjecting them to commercial manipulation and continuous surveillance; invading their privacy;
12 denying their due process rights by subjecting them to opaque, unreviewable data practices; forcing
13 them to choose between their right to an education and other fundamental rights; and failing to
14 compensate them for their property and labor.

15 327. Plaintiffs and Nationwide Class members did not consent to Padlet's taking of their
16 PI and using it for Padlet's or other third parties' commercial gain.

17 328. There is no justification for Padlet's enrichment. It would be inequitable,
18 unconscionable, and unjust for Padlet to be permitted to retain these benefits when they were
19 procured because of and by means of Padlet's wrongful conduct and at the expense of children's
20 property and wellbeing.

21 329. Plaintiffs and Nationwide Class members seek an order compelling Padlet to
22 disgorge the profits, data (including derivatives of the data and data used to train artificial-
23 intelligence models), and other benefits it has unjustly obtained.

24 330. Plaintiffs and Nationwide Class Members may not have an adequate remedy at law
25 against Padlet, and accordingly, they plead this claim for unjust enrichment in addition to, or in the
26 alternative to, other claims pleaded herein.

VIII. RELIEF REQUESTED

Wherefore, Plaintiffs respectfully request the Court enter judgment in their favor and against Padlet as follows:

- a. An award of damages, including actual, compensatory, general, special, incidental, consequential, and punitive damages, in an amount to be determined at trial;
- b. Injunctive, declaratory, and other equitable relief as appropriate;
- c. Pre- and post-judgment interest to the extent provided by law;
- d. Attorneys' fees to the extent provided by law;
- e. Costs to the extent provided by law; and
- f. Such other relief the Court deems just and proper.

IX. JURY TRIAL DEMAND

Plaintiffs demand a jury trial for all claims so triable.

Dated: September 14, 2026

/s/ Victor J. Sandoval

Victor J. Sandoval

ALMEIDA LAW GROUP LLC

Victor J. Sandoval (SBN 344461)

3415 S. Sepulveda Blvd. Suite 1121

Los Angeles, California 90034

(562) 534-5907

victor@almeidalawgroup.com

David S. Almeida (*pro hac vice* forthcoming)

Britany Wessan (*pro hac vice* forthcoming)

ALMEIDA LAW GROUP LLC

849 W. Webster

Chicago, IL 60614

david@almeidalawgroup.com

britany@almeidalawgroup.com

Julie U. Liddell (*pro hac vice* forthcoming)

julie.liddell@edtech.law

W. Andrew Liddell (*pro hac vice* forthcoming)

andrew.liddell@edtech.law

Elizabeth Huddleston (*pro hac vice* forthcoming)

beth.huddleston@edtech.law

EDTECH LAW CENTER PLLC

904 Rio Grande Street, Suite 100
Austin, Texas 78701
Tel.: (512) 200-8028

Brandon M. Wise (*pro hac vice* forthcoming)
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
314-833-4827
bwise@peifferwolf.com

Counsel for Plaintiffs and the Proposed Classes