Morgan D. Ross, Esq. (SBN 270650)
Robert B. Salgado, Esq. (SBN 297391)
COUNTERPOINT LEGAL
600 B Street, Ste 1550
San Diego, CA 92101
Tel: (619) 780-3303
Fax: (619) 344-0332
morgan@counterpointfirm.com
rsalgado@counterpointfirm.com

Attorneys for Plaintiffs and Putative Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

MICHAEL GARCIA, SALENA GARCIA, AND R.G., a minor by and through her guardians Michael Garcia and Salena Garcia, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

ROBLOX CORPORATION,

Defendant

Case No.: 30-2017-00908101-CU-RI-CXC

CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF FOR VIOLATIONS OF:

1. Electronic Communications Privacy Act (ECPA), Title I – Wiretap Act (18 U.S.C. § 2511)
2. The Stored Communications Act (SCA) (18 U.S.C. § 2701 *et seq.*)
3. The Children's online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6502, 6503, 16 C.F.R. Part 312)

JURY TRIAL DEMANDED

INTRODUCTION

Plaintiffs MICHAEL GARCIA, SALENA GARCIA and R.G. (collectively "Plaintiffs") individually and on behalf of all others similarly situated, by and through Plaintiffs' undersigned counsel, bring this class action lawsuit against ROBLOX CORPORATION ("Defendant" or "Roblox") and alleges, based upon information and belief and the investigation of Plaintiffs' counsel as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of a nationwide class of Roblox users to remedy systemic privacy violations by Defendant Roblox Corporation ("Roblox"). Roblox operates a massively popular online gaming platform frequented by millions of users—including a large percentage of children under 18. Unbeknownst to these users (or their parents), Roblox has been surreptitiously intercepting their electronic communications and harvesting detailed personal data through covert tracking code embedded in its website and apps. This data surveillance begins the moment a user visits or launches Roblox, even before account login or consent, and continues across platforms (web, iOS, Android, macOS, Windows) via persistent identifiers and fingerprinting techniques. Plaintiffs seek to hold Roblox accountable under federal law for these unlawful practices, including violations of the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (), and to enjoin Roblox's ongoing collection of children's personal information in violation of the Children's Online Privacy Protection Act (COPPA).

2. Roblox's conduct is both technically invasive and legally forbidden. Through hidden scripts and trackers, Roblox intercepts the contents of users' communications with its platform and shares them with third parties for analytics and advertising, without users' knowledge or consent. For example, Roblox's code executes canvas fingerprinting (using the HTML5 canvas to extract a unique device signature) and audio fingerprinting (using the Web Audio API to generate unique sound-based identifiers) immediately upon a user's visit and assigns unique tracking IDs that persist across sessions and devices, enabling the re-identification of users even after they log out or clear cookies. It logs detailed telemetry data—browser and device configuration, IP address, installed fonts/graphics details, mouse movements and keystrokes—then transmits this information to its servers and to partner domains in real time. These practices amount to an electronic

wiretap on every user interaction, in violation of ECPA's prohibition on intercepting electronic communications.

3. Critically, a huge portion of Roblox's user base are children, and Roblox's tracking targets minors with equal or greater intensity. Roblox knew that many users are under 13 (indeed, roughly 54% of Roblox's daily active users were 13 years of age and older, and 46% were under the age of 13)[1], yet it designed its platform to harvest children's personal information without obtaining verifiable parental consent. COPPA and its regulations expressly prohibit collecting a child's personal identifiers for anything other than internal operations without parental consent, but Roblox ignored these safeguards. The company's own policies acknowledge it engages in personalized advertising and cross-site tracking of users, meaning children on Roblox are being profiled by Roblox and its ad-tech partners unbeknownst to their parents. Roblox never provided parents with direct notice of these data practices nor sought parental consent, as required by COPPA. Thus, Roblox not only violated COPPA's provisions but also ensured that any "consent" defense it might claim under other laws (such as one-party consent under ECPA) is invalid due to its tortious and unlawful purpose.

4. Plaintiffs Michael Garcia and Salena Garcia are parents who, like millions of others, trusted Roblox to be a safe, child-friendly platform. They allowed their 12-year-old child, R.G., to use Roblox, unaware that Roblox would secretly record R.G.'s online interactions and device details. Had they known the truth—that Roblox would effectively spy on their child's activities and identity for profit—they would not have allowed R.G. to use the platform. Plaintiffs bring this action to stop Roblox's intrusive surveillance, to seek statutory damages for the class (including at least $10,000 per person under ECPA's liquidated damages provision), and to obtain injunctive and declaratory relief. Among other things,

[1] Roblox 10-k filing for fiscal year ended December 31, 2022, filed February 28, 2023, SEC Accession Number: 0001315098-23-000032.

Plaintiffs ask the Court to order Roblox to cease intercepting user communications without consent, delete all unlawfully collected data (particularly from children), and implement strict privacy safeguards and parental consent mechanisms going forward. Plaintiffs also seek punitive damages to punish Roblox's willful disregard of users' privacy rights, and an award of attorneys' fees and costs as provided by law.

5. In summary, Roblox engineered a pervasive tracking system that covertly eavesdrops on users across the Roblox platform. This lawsuit seeks to vindicate the class's rights under federal privacy statutes and to ensure that Roblox's young users can enjoy the service without being secretly watched and recorded at every step. The allegations below are supported by forensic evidence of Roblox's data collection in action, as detailed in the accompanying evidence appendix.

6. "Technological advances[,]" such as Defendant's use of "session replay" technology, "provide 'access to a category of information otherwise unknowable' and 'implicate privacy concerns' in a manner different from traditional intrusions as a 'ride on horseback' is different from a 'flight to the moon.'" *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)).

JURISDICTION AND VENUE

7. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this action arises under federal statutes, including the Electronic Communications Privacy Act (18 U.S.C. § 2510 et seq.) and the Stored Communications Act (18 U.S.C. § 2701 et seq.). The Court also has jurisdiction under 18 U.S.C. § 2520 (ECPA's civil action provision) and 18 U.S.C. § 2707 (SCA's civil action provision), which expressly authorize private suits. Additionally, the Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the proposed class consists of many thousands of users

across multiple states, minimal diversity is satisfied, and the aggregate amount in controversy exceeds $5 million.

8. The Court has personal jurisdiction over Defendant Roblox Corporation because Roblox is headquartered in California (San Mateo) and conducts substantial business within California, including in Los Angeles. Roblox purposefully avails itself of the California market by providing its platform to millions of California residents (including class members) and by engaging in the wrongful conduct alleged herein from California. The effects of Roblox's conduct were felt in California, where Plaintiffs used the service and where children's data was collected. Roblox has continuous and systematic contacts with California, rendering it essentially at home here.

9. Venue is proper in the Central District of California pursuant to 28 U.S.C. § 1391(b) and (c) because Defendant conducts substantial business throughout the State of California, including within this District, and because a substantial part of the events or omissions giving rise to the claims occurred in this District. Defendant maintains continuous and systematic contacts with this District, and the unlawful practices alleged herein were targeted to and affected consumers within this District. Although the named Plaintiffs reside in San Diego County, and Defendant is headquartered in San Mateo County, this action is brought on behalf of a statewide class of consumers, many of whom reside in the Central District. Accordingly, venue is proper in this District.

PARTIES

10. Plaintiff Michael Garcia is an adult individual and a resident of Los Angeles, California. He is the father and legal guardian of Plaintiff R.G., a minor child. Michael Garcia directly interacted with the Roblox platform in California – including downloading the Roblox app and supervising R.G.'s use of Roblox – and was himself subjected to Roblox's data collection practices when doing so. Michael Garcia brings this action on his own behalf (to the extent his own

electronic communications and personal data were retained by Roblox), and to vindicate his rights as a consumer and as a parent) and on behalf of his minor child, R.G. as guardian. Michael Garcia has a strong interest in protecting his child's online privacy and would not have allowed R.G. to use Roblox had he known of the hidden surveillance and tracking now at issue.

11. Plaintiff Salena Garcia is an adult individual and a resident of Los Angeles, California. She is the mother and legal guardian of Plaintiff R.G., the minor child in this action. Salena Garcia has also directly interacted with Roblox's platform in California, including visiting the Roblox website and assisting R.G. with setting up an account. In doing so, Salena Garcia was exposed to the same undisclosed data interception practices (for example, Roblox collected information from her browser when she visited the site). Salena Garcia joins this action on her own behalf and as a guardian on behalf of R.G. She, too, was misled about the nature of Roblox's platform and believed it to be safe for children. Salena Garcia's personal interests were affected because Roblox's conduct undermined her right to control the information collected from her child. Like Michael, Salena brings this case to safeguard her child's privacy and to hold Roblox accountable for violating both her and her child's rights.

12. Plaintiff R.G. is a minor child residing in San Diego, California. R.G. has used the Roblox platform regularly since approximately 2021 (from around age 9 or 10), accessing it via Roblox's website and mobile app to play games and socialize with friends. During all times relevant to this Complaint, R.G. was under the age of 13 and thus falls under the protections of COPPA as a child user. R.G. brings this action by and through her parents and legal guardians, Michael and Salena Garcia, because of the communications generated by R.G.'s Roblox usage – including device identifiers, game interaction data, chat messages, and other online activities – were intercepted, stored, and disseminated by Roblox without parental consent. R.G.'s interests in this litigation are represented by her parents, who seek

relief on her behalf to remedy the violations of R.G.'s statutory privacy rights.

13. Defendant Roblox Corporation ("Roblox") is a Delaware corporation with its principal place of business at 970 Park Place, San Mateo, California 94403. Roblox develops and operates the "Roblox" online platform, which consists of a website and applications that allow users to play and create games in a virtual space. Roblox's platform is accessible worldwide, including by users throughout California and this District, via web browsers and dedicated apps on iOS, Android, Windows, and macOS. Roblox's business model includes revenue from in-game purchases ("Robux" currency) and advertising/marketing partnerships that depend on collecting and exploiting user data. At all relevant times, Roblox acted through its employees, software engineers, and third-party agents (such as embedded analytics/advertising services), who carried out the alleged actions described herein within the scope of their agency and for Roblox's benefit. Roblox had actual knowledge that a significant portion of its users are children under 13, as evidenced by birthdate information collected at signup and its own public statements acknowledging its young user base. Despite this knowledge, Roblox engaged in uniform data interception practices across all users, including children, without adhering to legal requirements for children's privacy.

14. Plaintiffs are informed and believe that additional parties yet unknown to them may have liability for the acts alleged (for example, third-party analytics or advertising companies that actively participated in the unlawful collection and distribution of communications from Roblox users). These unknown actors are sued as Doe Defendants 1–10. Plaintiffs seek leave to amend this Complaint to name any such parties once their identities and involvement are ascertained through investigation or discovery. For purposes of this Complaint, all references to "Roblox" or "Defendant" encompass not only Roblox Corporation but also those acting in concert with it in implementing the challenged data collection scheme, unless otherwise indicated.

FACTUAL ALLEGATIONS

A. User and Usage Data Have Immense Economic Value

15. The "world's most valuable resource is no longer oil, but data.[2]

16. Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (i.e., customers' purchase histories, private interests, and product usage information), and attitudinal data (i.e., data on consumer satisfaction) from consumers.[3] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[4]

17. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[5]

18. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[6] In this paper, the OECD measured prices demanded by companies concerning user data derived

---

[2] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-nolongeroil-but-data.

[3] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businessescollecting-data.html.

[4] *Id*.

[5] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/businessfunctions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[6] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

from "various online data warehouses."[7]

19. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military record is estimated to cost USD 55."[8]

20. In more recent publications by the OECD, there is a documented shift in market strategies concerning the exploitation of consumer data. Rather than relying on traditional buy-sell models or isolated one-time data transactions, companies have increasingly transitioned toward monetizing data through the provision of data-driven services and the development of advertising ecosystems that leverage consumer information as a core revenue-generating asset. This evolution has allowed firms to retain control over data assets while maximizing long-term profitability by embedding data into the architecture of digital platforms and personalized advertising systems.[9]

21. n the rapidly expanding industry of data extraction from digital platforms, one-to-one data transactions—such as direct sales of consumer information—generated approximately USD 33.3 billion in revenue.[10] In contrast, data-driven internet advertising, which leverages user information for targeted marketing rather than direct sale, was valued at over USD 112 billion.[11]

B. Roblox's Platform and User Base

22. Roblox offers an interactive online platform that hosts countless user-created games and virtual experiences. Launched in 2006, the platform has grown

---

[7] *Id*. At 25
[8] *Id*.
[9] *Measuring the Value of Data and Data Flows*, OECD Digital Economy Papers, No. 345 (Dec. 2022), https://*www*.oecd-ilibrary.org/docserver/1ba5e5d5-en.pdf.
[10] *Id*. At 6
[11] *Id.* At 21

exponentially and is especially popular with children and teenagers. Users create accounts (often with avatars) and join games where they can chat and collaborate with others in real time. Roblox is free to join, which has helped it attract a huge youth audience; as of recent estimates, Roblox had over 50 million daily active users, and roughly 42% of these daily users are under 13 years old. By design, Roblox markets itself as a family-friendly, creative environment for children that provides age-appropriate content, and even allows accounts associated with children under the age of 13 to have certain chat filters. Roblox thus knows that children are a core demographic on its platform.

23. Whenever a user is active on Roblox, their device is constantly exchanging data with Roblox's servers. This data stream is what enables the dynamic gameplay and social features: for example, the user's device sends inputs (movements, chat messages, game actions) to the server and receives back data concerning the player's actions.

24. In essence, Roblox functions as an electronic communication service between users and Roblox's servers (and between users themselves in multiplayer games). Because of this continuous exchange, Roblox has access to virtually everything a user does on the platform, from text conversations to the unique technical fingerprints of the user's device connecting to the service. Roblox's privacy policy acknowledges collecting a wide range of user data (device identifiers, usage logs, etc.) ostensibly to improve services and safety. However, what Roblox does not adequately disclose is the extent to which it employs surveillance technologies to track users beyond what is necessary for gameplay or safety.

C. Roblox's Hidden Tracking and Data Collection Scheme

25. Forensic analysis reveals that Roblox has implemented a sophisticated, covert tracking apparatus across its platform. From the moment a user accesses Roblox's website or app, Roblox injects scripts that gather detailed device and

behavior information. This occurs ***whether or not*** the user ultimately creates an account or logs in. Some key aspects of Roblox's tracking scheme include:

a. **Device Fingerprinting**: Roblox's code runs multiple fingerprinting routines on the user's device upon page load or app launch. One method is canvas fingerprinting, which involves instructing the browser to draw hidden code in an HTML5 canvas element and reading back the pixel data to generate a unique hash signature of the user's graphics hardware and software. Another method involves **audio fingerprints**, whereby Roblox uses the Web Audio API to produce an inaudible sound signal and measure slight variations in the output (e.g., via an OfflineAudioContext and oscillator), creating a unique audio-based identifier. These fingerprinting processes are executed immediately and automatically, without any user action, and they yield persistent identifiers that can recognize the device on future visits even if cookies are cleared.

b. **Persistent Identifiers (UIDs)**: Beyond one-time or single-session trackers, Roblox assigns users a persistent unique identifier (or "UID") that persists across sessions and platforms. For example, evidence shows that Roblox generates values like a deviceUniqueID or RBXID/RBXSessionID and stores them in the browser's local storage or cookies. These identifiers are regenerated or synchronized such that even if a user logs out, uses a private browsing window, or reinstalls the app, Roblox can re-link them to their prior profile. In other words, Roblox's system defeats conventional privacy measures (clearing cookies, using incognito mode) by reproducing the same fingerprint and linking it to the same UID whenever the user returns. This allows Roblox to track an individual user's behavior over time and across different devices or browsers, effectively creating a cross-platform surveillance profile of that user.

c. **Telemetry and Behavior Capture**: Roblox monitors granular user

interactions and device telemetry beyond just necessary game data. For instance, Roblox's web interface attaches hidden event listeners to track user inputs like mouse movements, clicks, scrolling behavior, and keystrokes on form fields. This has been documented in developer console logs: each keystroke in a login or chat field is captured (with timing data) and sent to Roblox's servers even if the user never submits the form. Similarly, the platform measures things like cursor velocity or tap cadence (via Arkose Labs scripts used for "bot" detection) and phone sensor data, funneling that information into Roblox's data stream. All of this happens in the background under the label of "telemetry" or anti-fraud monitoring, but in reality it constitutes an expansive collection of personal behavioral data far beyond what a user would expect for gameplay.

d. **Immediate Data Transmission**: The data collected by these scripts is transmitted off the user's device in real time, often to Roblox-controlled analytics domains or directly to third-party servers. Notably, this transmission begins before any consent or even account login. For example, when a new visitor lands on Roblox's homepage or sign-up page, the site immediately makes network requests to domains like *ecsv2.roblox.com* (Roblox's analytics) and *ssl.google-analytics.com* (Google Analytics) containing fingerprint hashes, device info, and unique IDs. Plaintiffs' forensic investigation captured these network requests in HTTP Archive (HAR) logs and packet sniffer traces, confirming that personal device data is sent to Roblox and third parties within seconds of loading the page, before the user can even click "I agree" or learn of any privacy policy. In essence, Roblox intercepts the communication between the user and the website/app by diverting it to analytics endpoints simultaneously. The user's device is effectively sending a duplicate of its communications (like web requests, device handshake data, etc.) to unauthorized recipients orchestrated by

Roblox.

e. **Third-Party Trackers**: In addition to its own data collection, Roblox has integrated third-party tracking services that piggyback on the platform to gather user data. For instance, Roblox includes code from Google Analytics, which means that as users interact with Roblox, Google's servers are also silently receiving data about that interaction. Roblox also invokes scripts from Stripe (a payment processor) on pages that have no payment functionality, purely to leverage Stripe's device fingerprinting for fraud detection. Another example is Arkose Labs, a third-party "bot detection" vendor, whose scripts collect behavioral biometrics (mouse movements, typing rhythms, etc.) ostensibly to distinguish robots from humans. In practice, these third-party inclusions result in outside companies "listening in" on the user's communications with Roblox. Data that the user likely assumes is only going to Roblox's servers is simultaneously sent to domains controlled by Google, Stripe, Arkose, and potentially others, all without the user's knowledge. This arrangement effectively constitutes an ongoing wiretap, where Roblox has enabled third parties to eavesdrop on the data stream between users and Roblox.

26. Through the above mechanisms, Roblox builds a comprehensive profile of each user's device and activity. The profile can include technical fingerprints (canvas hashes, audio hashes, installed fonts, GPU and CPU traits), persistent IDs linking sessions, behavioral metrics (typing speed, clicking patterns), and context about the user's content (such as which games or pages they visit). Crucially, much of this information qualifies as the "contents" of communications or highly personal data. For example, the exact URL of a game page or the text of chat messages are contents of communications, and even the fingerprint data can be considered content when it reveals information about the user's system that is not address or routing data. Roblox's system captures this information

contemporaneously with the user's interactions, and it is designed to do so without alerting the user or giving any meaningful opportunity to consent.

D. Roblox's Use of Data and Third-Party Sharing

27. Roblox did not implement this extensive surveillance for benign or purely internal purposes. The data collected feeds into Roblox's monetization and growth strategy. By tracking users (including minors) across the platform and even across the internet, Roblox can increase user engagement and advertising revenue. Some specifics include:

a. **Personalization and Targeted Content**: Roblox uses the data to personalize the user's experience, which on its face sounds legitimate – e.g., recommending games a user might like. However, personalization based on covert tracking (especially of kids) can cross into manipulation and certainly goes beyond "internal operations." For instance, Roblox can analyze a child's play habits, chat activity, or even physiological responses (through biometric proxies like typing cadence) to predict what will keep them hooked and then adjust what content to show or which notifications to send. This algorithmic targeting is fueled by the rich data Roblox gathers surreptitiously.

b. Advertising and Marketing: Roblox has been increasingly integrating advertising into its platform. Its privacy disclosures (when carefully read) admit that personal information is shared with third parties for marketing and analytics. In practice, this means data about users (unique IDs, device fingerprints, behavioral profiles) may be shared with outside ad networks or partners who then use it to serve targeted ads or to track the user on other sites. The evidence indicates that Roblox operates a dedicated tracking domain rbxtrk.com for user data collection and also relies on mainstream trackers like Google Analytics. Thus, a child playing a game on Roblox could unknowingly have their information shared with external advertising networks that build a broader profile of that child across the web.

c. **Cross-Platform Profiling:** Roblox can link activity on a web browser to their activity on a mobile app, if it has correlated their device fingerprints and UIDs. This means even if a user (or parent) tries to delete or reset an account, Roblox can recognize the returning user. The company effectively follows users from device to device, ensuring that the data profile (and any advertising targeting based on it) persists. This has special implications for children who might use a parent's device or switch between a school computer and a home tablet—Roblox's tracking could potentially connect all those sessions together.

d. Data Stored and Sold/Shared: All intercepted data is stored on Roblox's servers (and possibly on third-party servers like Google's). While Roblox claims in its terms that it does not "sell" personal data, the reality is that sharing for analytics or advertising can be a sale under various laws. Regardless of terminology, collection and external sharing of kids' data without consent is exactly what COPPA and other privacy laws were designed to prevent. The harm is not only theoretical: children on Roblox are being profiled in ways that could influence in-game content, expose them to targeted ads, or even risk their data being re-identified or misused if there were a security breach or if third parties use it for unintended purposes.

E. Lack of Consent and Parental Awareness

28. At no point do Roblox users—or parents of minor users—give informed consent to this breadth of data collection. Roblox's user interface provides no clear warning that by using the platform, the user is subject to extensive tracking. When a user (even a child) creates an account, or even visits the website, they are immediately being tracked. At no point is the user ever given a disclosure about the nature of the tracking or presented with a screen where they are able to provide any meaningful consent or permission.

29. General Terms of Service and a Privacy Policy link; there is no granular

opt-in for data tracking or any mention of ongoing surveillance of communications. Importantly, minors cannot legally consent, and Roblox's onboarding does not involve any parental consent mechanism for data collection. Upon the conclusion of a new account's session -prior to signing our – a user will be prompted to provide a recovery email, for a minor it will request a parental recovery. Roblox's only gesture toward COPPA compliance in this context is the delivery of its "Roblox Terms" to the provided parental email address *after* the minor has already accessed and engaged with the platform. At no point prior to the collection of the child's personal information does Roblox obtain verifiable parental consent

30. Roblox's Privacy Policy (which most users, especially children, are unlikely to read) does disclose in broad terms that Roblox collects device identifiers, usage info, and may use it for improving services or safeguarding their users while in-game, but it downplays or fails to reveal the invasive specifics like fingerprinting or third-party sharing for advertising. In fact, independent analyses of Roblox's privacy practices have noted that parental consent is not required before personal information is collected or disclosed by Roblox, despite the company's awareness of their under-13 users. This indicates a willful decision by Roblox to ignore parental consent obligations. By structuring its data harvesting to run automatically and silently, Roblox ensured that the average user would remain oblivious. A child simply sees their game loading normally, unaware that behind the scenes their device just sent a trove of data to various servers — data they cannot legally consent to share in the first place, as minors lack the legal capacity to provide informed consent.

31. The lack of consent is not only a matter of missing user agreement; it ties into the tortious purpose of Roblox's interception. Under ECPA, even if one party (here Roblox) could argue it was a party to the communication and "consented" to the interception, that consent is invalid if the interception is done

for the purpose of committing a crime. As detailed below, Roblox's purpose included violating COPPA (a law carrying civil penalties for collecting children's data without consent) and committing a broad intrusion upon the privacy of its users. Roblox cannot now claim that users implicitly consented via terms of service or that Roblox itself consented to monitor its communications is improper. Plaintiffs and class members certainly never agreed to be wiretapped or tracked in this pervasive manner, and any theoretical consent extracted via a standard clickwrap agreement was not informed and is void as to these specific practices.

F. Impact on Plaintiffs and Class Members

32. Roblox's conduct has caused harm to Plaintiffs and the class. Each class member's statutorily protected privacy rights under ECPA and the SCA were violated the moment Roblox intercepted their communications or accessed their data without authorization. These are concrete injuries recognized by law – Congress set statutory damages exactly because such privacy intrusions are harmful. Beyond the statutes, the intrusion upon seclusion suffered by Plaintiffs (especially minors) is highly offensive to a reasonable person. Plaintiffs had a reasonable expectation that their private communications (and their devices' intimate details) would not be secretly taped and recorded for profit. Roblox shattered those expectations by imposing their data collection methods on users in a manner akin to installing a surveillance bug on their personal device.

33. For minor users like R.G., the harm is particularly acute. Children are less aware of privacy risks and more vulnerable to manipulation in that Roblox's tracking could lead to manipulative targeting or profiling of children, shaping their online experience in unseen ways. Moreover, the unauthorized creation of a persistent profile on a child carries the risk of that data being misused or even breached, exposing the child to potential safety issues. Parents like Michael and Salena Garcia have suffered harm in that their parental rights to control the collection of their child's information were ignored. They have also experienced

anxiety and distress upon discovering that Roblox was surreptitiously collecting data from R.G. and from their own devices. Had they known, they would have taken steps to prevent or limit Roblox's use of their personal data or by using technical means to block trackers. Thus, they were deprived of the ability to make informed decisions about their and their child's privacy.

34. Economically, while Plaintiffs do not need to prove monetary loss for these causes of action, it is worth noting that Roblox unjustly profited from its wrongdoing. Roblox's data practices likely increased user engagement (and thereby revenue) and advertising effectiveness. Plaintiffs (like many class members) also spent money on Roblox (purchasing "Robux" currency) during the class period. If Plaintiffs had known their communications were being intercepted and their child's data exploited, they would not have supported the platform financially. The data collected from users has inherent value as well – value that Roblox monetized without any compensation to users. These considerations reinforce that a remedy is needed not just to compensate class members but to disgorge Roblox's ill-gotten gains for their flagrant violations.

STANDING

35. Defendant's conduct constituted invasions of privacy because it disregarded Plaintiff's statutorily protected rights to privacy, in violation of CIPA, SCA, the Wiretap Act, and COPPA.

36. Defendant caused the Plaintiffs to 1) suffer invasions of legally protected interests. The invasions were concrete because the injuries actually existed for the Plaintiffs and continue to exist every time the Plaintiffs use the Roblox platform or visit the Roblox website. The privacy invasions suffered by the Plaintiffs and Class Members are real and not abstract. Plaintiffs and Class Members have a statutory right to be free from interceptions of their communications. The interceptions Defendant performed were meant to secretly spy on the Plaintiffs and their children in an effort to learn more about their behavior. Plaintiffs and Class

Members were completely unaware they were being observed to this extent. Plaintiff's injuries were not divorced from concrete harm in that privacy has long been protected in the form of trespassing laws and the Fourth Amendment of the U.S. Constitution, for example. Like here, an unreasonable search may not cause actual physical injury, but is considered serious harm, nonetheless. The injuries here are particularized because they affected the Plaintiffs in personal and individual ways. While the injuries were individualized rather than collective, the intrusive data collection policies and practices used by Roblox are widespread and apply to all Plaintiffs and class members. Roblox's past invasions are still ongoing and are imminent and will and do occur each and every time an individual visits their website, plays their video game or socializes with other players. Defendant continues to intercept communications without consent and will continue to do so unless and until a favorable decision by this Court is made that would redress the injuries of the Plaintiffs and the proposed class and subclasses.

TOLLING

37. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that their information was intercepted, because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

38. Plaintiffs bring this lawsuit as a class action on behalf of the Plaintiffs and members of the proposed class and subclasses under F.R.C.P. 23.

39. **Class Definition**: Plaintiffs seek to represent a nationwide "Class" defined as: "All persons within the United States who used the Roblox platform (website or apps) at any time from July 1, 2021, to the present." Included in the Class are both minors and adults who went onto any and all Roblox web platforms or applications during the class period. Excluded from the Class are: (a) Roblox Corporation and its officers and employees; (b) any Judge or Magistrate presiding over this action and their immediate family members; and (c) any individuals who

timely opt out of the Class. Plaintiffs reserve the right to modify the class definition or propose subclasses as appropriate after further investigation and discovery.

40. **Subclass – Minor Users**: Plaintiffs propose a subclass of Minor Users (the "Minor Subclass"), defined as: All Class members who used the Roblox platform while under the age of 18 (including those who are still minors and those who have since reached adulthood, for claims arising from their under-18 usage). This subclass is particularly important for addressing issues unique to minors, such as COPPA-related violations and limitations on consent. Plaintiff R.G. (through her parents) is a representative of this Minor Subclass, and her claims are typical of other minor users' claims.

41. **Subclass – Adult Users**: Plaintiffs also propose a subclass of Adult Users (the "Adult Subclass"), defined as: "All Class members who used the Roblox platform while age 18 or older." This subclass addresses the fact that adults (or users who have reached adulthood during the class period) are also victims of Roblox's interception and data collection, even though COPPA may not apply to them. Plaintiffs Michael and Salena Garcia are representatives of the Adult Subclass, as each has used Roblox as an adult and suffered the alleged violations.

42. **Numerosity**: The Class and subclasses are so numerous that joinder of all members is unfeasible and impracticable. Roblox's user base in the U.S. numbers in the many millions. For example, by one estimate there were over 32 million users under 13 worldwide as of recent years, and tens of millions of users in the U.S. overall. Even a conservative slice of U.S. users during the class period would yield hundreds of thousands or millions of individuals affected. The members of the Class are geographically dispersed across the United States. The precise number of Class members can be ascertained from Roblox's records (account registrations, device fingerprints, etc.), but it is far beyond what would be manageable in individual lawsuits.

43. **Commonality**: There are numerous questions of law and fact common to the Class that can be answered on a class-wide basis, including:

a. Whether Roblox, through the design of its website and apps, intercepted or caused to be intercepted electronic communications of users without consent (e.g. by duplicating user data to third-party analytics).

b. Whether the data Roblox collected included the "contents" of communications (as defined in ECPA) such that ECPA's Wiretap Act applies.

c. Whether Roblox's conduct violated the federal Wiretap Act (ECPA, 18 U.S.C. § 2511) by intentionally intercepting electronic communications.

d. Whether Roblox's conduct violated the Stored Communications Act (18 U.S.C. § 2701 et seq.) by unlawfully accessing, obtaining, or divulging electronic communications or records stored in an electronic medium.

e. Whether any exceptions or defenses (such as consent or ordinary course of business) apply to the interceptions, or whether such defenses are negated by Roblox's purpose to commit a tortious or unlawful act (including COPPA violations and invasion of privacy).

f. Whether Roblox collected "personal information" from children under 13 years of age without obtaining verifiable parental consent, in violation of COPPA.

g. Whether Roblox had actual knowledge that it was collecting personal information from children under 13 (e.g., through birthdate data) and yet failed to comply with COPPA's requirements.

h. Whether class members are entitled to statutory damages under ECPA (18 U.S.C. § 2520) and in what amount (e.g., $10,000 per person or $100 per day of violation).

i. Whether class members are entitled to statutory damages under the SCA (18 U.S.C. § 2707), including a minimum of $1,000 per person for willful violations.

j. Whether injunctive relief is appropriate to enjoin Roblox from continuing the alleged practices and to require deletion of unlawfully obtained data.

k. Whether the Court should declare that Roblox's conduct as alleged violated ECPA, SCA, and COPPA.

l. Whether Roblox acted willfully or with reckless disregard for the law and users' rights, such that punitive damages are warranted.

44. These common questions have answers that will drive the resolution of the litigation for all Class members. The evidence concerning Roblox's system design and conduct is common to all users; it is not dependent on an individual's circumstances. For example, either Roblox's code intercepted communications or it did not – and forensic evidence shows it did, uniformly. Whether a given data packet constitutes "contents" or whether consent was obtained are legal/factual questions that apply class-wide, not turning on any unique interaction of a particular user. Thus, the core issues are common.

45. **Typicality**: The claims of the representative Plaintiffs (Michael Garcia, Salena Garcia, and R.G.) are typical of the claims of the Class and subclasses. Each class member's claim arises from the same course of conduct by Roblox – the surreptitious interception of their communications and data through the Roblox platform – and each asserts the same legal theories (violations of ECPA, SCA, etc.). The specific harm to the Garcias and R.G. (loss of privacy, unauthorized data collection) is the same harm experienced by all class members. There may be minor factual variations (e.g., one user might have used only the web version, another mostly the mobile app), but Roblox's tracking was present on all platforms and will be shown to function similarly across them. Thus, proving the named Plaintiffs' claims will also prove the claims of the Class. Plaintiffs have no interests antagonistic to other Class members; on the contrary, they share the primary goal of stopping Roblox's unlawful conduct and obtaining relief for all

affected.

46. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the Class. Michael and Salena Garcia, as parents, are dedicated to protecting not only their child but all children and users on Roblox who suffered from these practices. They have no conflicts of interest with the Class. They understand the obligations of class representatives and have retained counsel experienced in complex privacy and class action litigation. Plaintiffs' counsel will vigorously prosecute the case on behalf of the Class, having experience with technology-focused privacy cases. There is no disabling conflict between Plaintiffs and any subclass either – indeed, by having both adult and minor represented, the interests of both groups are accounted for. All Class members seek the same outcomes: a finding of liability against Roblox, monetary statutory damages, and appropriate injunctive relief.

47. **Predominance and Superiority**: Common questions of law and fact predominate over any questions affecting only individual members. The key legal issues (Roblox's liability under ECPA and SCA, COPPA non-compliance) do not require individualized proof. The measure of statutory damages is essentially set by statute per person, not requiring individualized calculations of harm. To the extent any minor differences exist (such as the age of the user or the number of days they used Roblox), those can be managed in the damages phase or by subclassing, and they do not overwhelm the common issues. Given the relatively modest statutory damages per person (e.g., $10,000 under ECPA, $1,000 under SCA) compared to the resources of a large company like Roblox, a class action is the superior method to adjudicate these claims. If each user had to sue Roblox individually, few would be able or willing to do so, especially minors. A class action ensures all injured users, including children, can obtain relief with efficiency and consistency. Class treatment also avoids the risk of inconsistent judgments that could arise from piecemeal litigation.

48. **Ascertainability**: Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's own logs, records and user contact information.

49. Furthermore, this case is manageable as a class action. The evidence of Roblox's conduct is largely in its source code, network logs, and corporate records, which apply to the class as a whole. Damages under the statutes are standardized. Notice to class members can be given through Roblox's own user contact info (emails on account, etc.). There is no known difficulty in maintaining this suit as a class action. This Court is an appropriate forum and concentrating the litigation here is beneficial because much of the conduct occurred in California and Roblox is based here.

50. Accordingly, Plaintiffs seek to certify the Class and the Minor and Adult Subclasses under Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Injunctive relief is appropriate on a class-wide basis (Rule 23(b)(2)) because Roblox has acted on grounds generally applicable to the class (instituting uniform tracking on all users), making a single injunction or declaratory judgment applicable to all. Monetary relief in the form of statutory damages also warrants class treatment (Rule 23(b)(3)) as common issues predominate and class resolution is superior.

FIRST CAUSE OF ACTION

Violation of the Electronic Communications Privacy Act (ECPA), Title I – Wiretap Act

(18 U.S.C. § 2511 – Unlawful Interception of Electronic Communications)

51. Plaintiffs reallege and incorporate by reference all preceding paragraphs as though fully set forth herein.

52. **Electronic Communications**: The interactions of Roblox users with the platform involve "electronic communications" within the meaning of 18 U.S.C. § 2510(12). Section 2510(12) defines an electronic communication to include any

transfer of signs, signals, writing, images, data, or intelligence of any nature transmitted by a wire, radio, electromagnetic, photoelectronic or photooptical system. Here, when users connect to Roblox's servers via the internet, they send and receive data (such as HTTP requests, WebSocket messages, chat messages, etc.) over wires and wireless networks, constituting electronic communications. For example, when Plaintiff R.G.'s browser loaded the Roblox home page, it sent a series of HTTP GET requests to Roblox's web server, transmitting information like the page URL and cookies. Similarly, when R.G. typed a message to a friend in a game, that chat text was transmitted as an electronic signal to Roblox's servers. These are all electronic communications. The contents of those communications include information concerning the substance or meaning of the communication (18 U.S.C. § 2510(8))—for instance, the actual text of a chat message or the specific resource a user is requesting on the website (which reveals what game or page they are viewing). Even seemingly technical data like a URL path or search query reveals content (e.g., a user searching for "Adventure Game" on Roblox has that search term as content). This case involves Roblox intercepting such contents.

53. **Interception by Device or Software**: Under 18 U.S.C. § 2511(1)(a), it is unlawful to intentionally intercept any electronic communication. "Intercept" is defined in § 2510(4) as the acquisition of the contents of a communication through any electronic, mechanical, or other device. Roblox violated this provision by intentionally intercepting the electronic communications between users and Roblox's platform. Specifically, Roblox designed and deployed software code as an intercepting "device" to divert portions of the communications stream to itself and third parties for unauthorized purposes. This occurred in several ways.

a. **Client-Side Duplication**: Roblox's web and app code caused users' devices to send copies of communications to unintended recipients. For example, when a user's browser made a request to load a game page,

Roblox's embedded Google Analytics script caused the browser to simultaneously send a duplicate request (containing the same URL and user ID info) to Google's servers. In doing so, the contents of the communication (what page was being accessed) were acquired by a third party in transit. Similarly, telemetry beacons (like the ecsv2.roblox.com calls) would package up information about the user's actions and device at the moment of interaction and send it off, effectively "tapping" the communication stream.

b. **Server-Side Interception**: Alternatively, or additionally, Roblox's own servers intercepted communications by splitting or redirecting data once it arrived. For instance, when Roblox's server received a user's data packet (an electronic communication), it may have automatically forwarded a copy to its analytics database or to a partnered service for analysis. From the user's perspective, their communication was intended for Roblox's service (to enable gameplay or chat), but Roblox diverted those communications (or data derived from them) to unauthorized uses like marketing analysis – a practice analogous to a phone operator listening in and forwarding a call's contents to a third party. The effect is the same as a contemporaneous interception during transmission.

c. **Integrated Sniffing Tools**: Roblox also integrated what are essentially packet-sniffing tools into the client, capturing user input before it is fully sent or processed. For example, the keylogging evidence shows Roblox's script capturing keystrokes as they are typed (even prior to form submission) and sending that data out. This means communications (like the content a user is typing) are acquired in real-time by Roblox's code running on the client device, which qualifies as an intercepting device. In sum, Roblox procured and used various devices (software modules like bundleVerification.js, metrics-runtime.js, analytics SDKs, etc.) to intercept communications contemporaneously with transmission.

54. Plaintiffs allege that **at least one if not all** of the above methods were employed by Roblox intentionally to intercept class members' communications. For instance, forensic network logs show that when J.D. (Plaintiff R.G.) was using Roblox, numerous requests were sent to third-party domains (such as Google Analytics and Roblox's own tracking subdomains) carrying information about the web pages visited and user identifiers. These transmissions occurred at the same time as, or immediately after, communications with Roblox's main servers, indicating a tap on the line. Therefore, an "interception" took place within the meaning of the Wiretap Act.

55. **Contents of Communications Intercepted**: The intercepted data included the contents of electronic communications. Under § 2510(8), "contents" includes any information concerning the substance, purport, or meaning of a communication. In this case, the things Roblox intercepted were not mere addressing or routing signals; they revealed substantive information about user communications. Examples include: the text of chat messages or forum posts (if those were monitored by analytics code), search terms entered by users on the platform, the specific game or profile page a user was viewing (which reveals what the user is interested in or doing), and even keystroke content (like characters of a password or message as typed, before encryption or send). One concrete example: Suppose a child user searched for a game called "ScaryMaze" on Roblox's search bar. That search query is an electronic communication from the user to Roblox's servers. If Roblox's tracking code sends that query to an analytics endpoint (to log popular search terms or feed its recommendation algorithm), then the content (the term "ScaryMaze") has been intercepted and acquired by a device not intended by the user (the analytics logger). Similarly, if a user's chat message or in-game voice data was captured by a third-party (for moderation AI or otherwise) in transit, that would be content interception. The forensic evidence, including HAR (HTTP Archive) files, will show specific instances where content like URL paths, page

titles, and user actions were included in intercepted data packets. Thus, the "contents" requirement of an ECPA violation is satisfied.

56. **Intentional Conduct**: Roblox acted intentionally in designing and executing this interception scheme. The deployment of tracking scripts and the routing of data to third parties was not accidental or incidental to providing the service—it was deliberately implemented to collect information. Roblox integrated these mechanisms fully aware that they would capture communications (they are standard analytics/tracking practices, not debugging tools). The company's motive was to gather data for profit and insight, which demonstrates the required intent: Roblox knew it was acquiring communication contents and did so on purpose. Any suggestion that these interceptions were part of normal operations is belied by their surreptitious nature and focus on marketing/analytics rather than the user-requested service (gameplay). Thus, Roblox intentionally intercepted electronic communications of users.

57. **Procurement and Aiding/Abetting**: In addition to directly intercepting communications, Roblox is liable under § 2511(1)(a) and (b) for procuring other persons to intercept and for aiding and abetting interceptions. Roblox embedded third-party tracking code (like Google Analytics, Stripe, Arkose Labs scripts) into its platform, effectively outsourcing the interception to those entities. By including that code, Roblox procured those third parties to intercept communications between users and the platform. For example, Roblox's deliberate addition of Google Analytics means Google was automatically intercepting data about users' usage. Roblox encouraged and facilitated this by design, making it just as responsible as if it did it itself. Moreover, even if those third parties are considered separate interceptors, Roblox is vicariously and secondarily liable: it aided and abetted their violations by providing the means and permission to collect the data. In this action, Plaintiffs focus on Roblox as the primary wrongdoer orchestrating everything but reserve the right to assert that these third parties also violated

ECPA. The key point is Roblox cannot escape liability by pointing to another actor—the law accounts for those who induce interceptions as well.

58. **Absence of Consent**: The interceptions occurred without the consent of any party to the communication, except perhaps Roblox itself. Neither Plaintiffs nor Class members gave prior consent to these interceptions. No user was ever asked to consent to having their communications monitored for third-party analytics or finger-printer tools. Roblox's Terms of Use and Privacy Policy did not explicitly disclose that the contents of interactions would be shared in real time with others, and certainly did not obtain users' affirmative agreement to such. Courts have held that for consent to be valid in the context of hidden website tracking, the user must have had specific notice of the interception; that was absent here. Additionally, minors like R.G. cannot legally consent to the interception of their communications—only a parent could, and no parent was meaningfully informed or asked. Thus, user consent is lacking.

59. Roblox might argue that it had consent because it was technically a party to every communication (as the provider receiving the data). Under ECPA's "one-party consent" rule (§ 2511(2)(d)), if one party to the communication consents, that can be a defense. Here, Roblox cannot use its own participation to bootstrap consent, for multiple reasons. First, as explained, the purpose of the interceptions was to commit tortious and unlawful acts, namely, to violate users' privacy and to infringe COPPA's protections. ECPA's one-party consent exception does not apply if the interception is done for the purpose of committing any criminal or tortious act (18 U.S.C. § 2511(2)(d)). Roblox's actions meet that exception: collecting children's data without parental consent violates COPPA (a law enforced by the FTC with civil penalties, and the knowing violation of which is wrongful). It also constitutes the tort of intrusion upon seclusion under common law. Therefore, even if Roblox contends it "consented" to the interceptions as a party, such consent is nullified by its tortious intent. Second, one cannot consent to

an illegal act that victimizes someone else – Roblox being a party doesn't mean the user's rights vanish. Particularly for minors, Roblox's claim of self-consent is dubious because COPPA effectively says the only valid consent for a child's data is from a parent. Roblox did not have that, so it cannot claim it had consent to intercept children's communications.

60. Improper Purpose (Tortious Act): Plaintiffs explicitly allege that Roblox's interception was done to further wrongful acts. The interceptions were inextricably linked to Roblox's violation of COPPA and other privacy laws. Roblox knowingly profiled children to enhance its profits, which is a purpose that contravenes public policy and statutory law. Internally, Roblox likely knew it should not be tracking kids in this manner (as discovery may show from communications or the need to keep these practices hidden). This demonstrates the kind of culpable intent that disqualifies any argument of innocent intent. The Wiretap Act's legislative history indicates that Congress wanted to prevent companies from self-excusing interceptions by claiming they were a party when they intercept for improper reasons – that is exactly the scenario here.

61. Damages Under ECPA: Section 2520 of ECPA provides that any person whose electronic communication is intercepted can recover civil damages and other relief. The statute sets liquidated or statutory damages as the greater of $10,000 per person or $100 per day of violation, for each plaintiff, along with potential punitive damages and attorney's fees (18 U.S.C. § 2520(c),(b)). Plaintiffs and Class members elect to recover the statutory damage amount for each person, as it is likely larger (and far easier to calculate uniformly) than actual damages. Each Class member is entitled to at least $10,000 in damages from Roblox for the interceptions. Given that many Class members (especially children) used Roblox frequently over a long period, the alternative $100 per day measure could in some cases exceed $10,000 – for example, a user who used Roblox on 200 separate days could claim $20,000. Plaintiffs reserve the right to demonstrate such extended

usage for some class members and seek higher statutory damages for them if supported, but for class-wide relief, $10,000 per person is a reasonable and minimally sufficient amount. With millions of class members, the total damages at stake are substantial, but that is a direct result of Roblox's broad misconduct. In addition to these statutory amounts, the Court may award punitive damages if it finds Roblox's interception was willful or malicious, and attorney's fees and costs are mandated to a prevailing plaintiff. Plaintiffs seek all such amounts as appropriate.

62. **Injunctive and Equitable Relief**: In addition to damages, ECPA authorizes "such preliminary and other equitable or declaratory relief as may be appropriate" (18 U.S.C. § 2520(b)(1)). Plaintiffs, on behalf of the Class, seek injunctive relief to stop Roblox's ongoing interceptions. Roblox's system continues to operate and will intercept communications from new and existing users every day until enjoined. The requested injunction would, at minimum: prohibit Roblox from embedding any code or third-party content in its platform that intercepts communications or tracks users without obtaining lawful consent, require Roblox to halt data transmission to any third-party analytics or advertising services unless and until users opt in, and require Roblox to implement a functioning consent mechanism (especially for minors, via parents) before any data beyond what is strictly necessary for service operation is collected. The injunction should also ensure Roblox deletes or sequesters any data already collected through illegal interception, to prevent ongoing use of ill-gotten data. Given the real-time, continuing nature of the violations, such injunctive relief is necessary to prevent irreparable harm (monetary relief alone cannot undo the privacy invasion for future communications).

63. Plaintiffs further seek declaratory relief under 28 U.S.C. § 2201, to have the Court declare that Roblox's conduct as alleged herein violates the ECPA. A declaratory judgment will serve the useful purpose of clarifying the law and

Roblox's obligations going forward, and it will reinforce to the industry at large that these kinds of secret wiretaps are illegal.

64. **Punitive Damages**: Roblox's actions were willful, wanton, and in conscious disregard of Class members' rights. Roblox is a sophisticated company that knew or should have known that wiretapping users (especially children) without consent was wrongful. The company nonetheless pursued this course to gain business advantages. This level of culpability warrants punitive damages under § 2520(b)(2), which allows punitive damages for willful or intentional violations in appropriate cases. Punitive damages are necessary here to punish Roblox (given its size and revenue, statutory damages alone may not suffice as a deterrent) and to deter similar conduct by others in the tech industry. Plaintiffs request that the amount of punitive damages be determined by the jury or Court at trial but note that it should be substantial in light of Roblox's egregious conduct and large user base (potentially a multiplier of the aggregate class recovery or another measure that ensures a meaningful penalty).

SECOND CAUSE OF ACTION

Violation of the Stored Communications Act (SCA)

(18 U.S.C. § 2701 et seq. – Unlawful Access to and Disclosure of Stored Electronic Communications)

65. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

66. **Electronic Storage and Service Provider**: The Stored Communications Act (SCA), 18 U.S.C. § 2701(a), makes it an offense to intentionally access, without authorization, a facility through which an electronic communication service (ECS) is provided, and thereby obtain access to electronic communications in electronic storage. Additionally, 18 U.S.C. § 2702(a) prohibits an ECS provider from knowingly divulging the contents of a communication while in electronic storage, to anyone other than the intended recipient, without authorization. In this

case, Roblox provides an electronic communication service to its users – it offers the ability to send or receive communications (messages, data, etc.) between users and between users and its servers, in connection with the platform's interactive features. Roblox's servers and databases are a "facility through which an electronic communication service is provided." When users send communications (like chats or game data) to Roblox's servers, those communications may be stored momentarily or for longer periods on Roblox's systems (for example, chat logs might be stored for moderation, game state data cached, etc.). Such data residing on Roblox's systems constitutes communications in "electronic storage" as defined by 18 U.S.C. § 2510(17) (which includes temporary, intermediate storage incidental to transmission and storage for purposes of backup).

67. **Unlawful Access and Exceeding Authorization (18 U.S.C. § 2701)**: Roblox, by engaging in the extensive data collection described, accessed communications in storage on its own servers and on user devices in a manner that exceeded authorization. Specifically, when users communicate with Roblox's service, they implicitly authorize Roblox to access and use those communications only for legitimate service purposes (such as delivering the game content or facilitating user chats to their intended recipients). Roblox exceeded any authorized access by mining those communications and associated data for additional purposes (analytics, profiling, sharing with partners) that were not necessary to provide the service and not consented to by the users. For example, if Roblox stored a user's chat message on its server for a moment to deliver it to another user, that's authorized. But if Roblox then accessed that stored chat message to analyze it for marketing trends or to feed an ad-targeting algorithm, that is an access of the stored communication beyond what the user permitted. Similarly, Roblox collects and stores detailed device logs and telemetry from user sessions. The user did not authorize Roblox to comb through those stored logs for purposes unrelated to the game (like selling insights or improving ad engagement). By doing so, Roblox

obtained access to communications in storage without user authorization, in violation of § 2701.

68. Additionally, Roblox effectively accessed data stored on users' own devices (such as browser local storage, cookies, or cached app data) by using scripts to retrieve identifiers or fingerprints. A user's device can be considered a "facility" that stores electronic communications (for instance, a browser's cache or local storage may hold tokens or messages as part of the service flow). Roblox's code that pulled persistent identifiers from local storage, even after logout or in private mode, was an access without authorization to data stored in a facility (the user's device) providing an electronic communication service. Users did not authorize Roblox to reach into their device storage beyond standard cookies for login, and certainly not to resurrect IDs after they've attempted to clear them. Thus, to the extent the SCA applies to client-side storage, Roblox exceeded authorized access there as well.

69. Unlawful Disclosure (18 U.S.C. § 2702): Roblox is also subject to § 2702(a)(1), which prohibits a person or entity providing an electronic communication service to the public from knowingly divulging to any third party the contents of any communication while in electronic storage by that service. Here, Roblox operates an ECS (as described) offered to the public (millions of users). When Roblox intercepted and stored communications (like the data packets and messages from users), those communications were in its electronic storage (even if briefly). By then channeling that information to third parties such as Google, Stripe, or others, Roblox knowingly divulged the contents of stored communications to persons not intended to receive them. For instance, if a user's HTTP request to Roblox (which might include a URL path indicating the game name) is temporarily in Roblox's server memory (storage) and Roblox forwards that to Google Analytics, Roblox has divulged contents (the URL/game info) to a third party without the user's consent. Another example: Roblox likely retains chat

logs or user-generated content on its servers for moderation/back-up. If Roblox allowed any third-party plugin or employee not involved in providing the service to sift through those logs for data, that would be a direct and willful violation.

70. Roblox likely retains chat logs or user-generated content on its servers for moderation or backup. If Roblox allowed any third-party plugin or external service to scan those stored chat logs for analytics (beyond the communication's intended recipients), that constitutes an unauthorized disclosure of communications in storage. In all such cases, Roblox knowingly divulged communications to third parties not authorized by the user, violating § 2702(a)(1).

71. **Lack of Lawful Authorization or Consent**: No SCA exception justifies Roblox's conduct. Users did not consent to Roblox accessing their stored communications for these secondary purposes, nor to Roblox sharing their communications with others. While service providers may access communications as necessary for the service or to protect their rights (§ 2701(c)), Roblox's pervasive data mining was not necessary for providing the Roblox game service – it was done for marketing and analytics, which is outside the scope of any authorization given by users. Likewise, the "protection of property" exception does not cover broad tracking of all users; at best, it might cover anti-fraud measures, but Roblox's wholesale data collection (especially from children) far exceeded any narrow anti-fraud necessity. Thus, Roblox's actions were without authorization and exceeded any authority it had.

72. **SCA Damages and Relief**: The SCA provides a civil cause of action (18 U.S.C. § 2707) for any person aggrieved by a violation of the statute. Roblox's violations of §§ 2701 and 2702 aggrieved Plaintiffs and Class members by infringing upon their privacy in stored communications. Under § 2707(c), a plaintiff is entitled to recover the greater of their actual damages and any profits made by the violator, or statutory damages of at least $1,000 per person. Plaintiffs and the Class seek statutory damages of $1,000 for each Class member (or for each

violation if deemed appropriate) for Roblox's willful and intentional violations of the SCA. Given the large number of Class members, the total statutory damages will be significant, but this reflects the scale of the wrongdoing. Additionally, because Roblox's conduct was deliberate, the Court may award punitive damages under § 2707(c) in its discretion. Plaintiffs request punitive damages to the extent necessary to punish and deter Roblox's conduct, especially since it involved exploitation of children's data. The SCA also mandates an award of reasonable attorneys' fees and litigation costs to a prevailing party (§ 2707(b)(3)), which Plaintiffs seek on behalf of the Class.

73. Plaintiffs further seek **appropriate equitable relief** under the SCA. The statute allows for injunctive relief as the court may deem appropriate (§ 2707(b)(1)). In this case, overlapping with the ECPA injunctive relief, Plaintiffs ask for an order requiring Roblox to delete or sequester all communications and data it collected from users in violation of the SCA and to cease any ongoing practices that involve accessing or sharing stored user communications without consent. This includes an order to stop sharing any user content or data with third parties except as lawfully authorized by users or as required for the core service. Such relief is necessary to ensure that data wrongfully obtained is not further misused and that Roblox conforms its conduct to the law going forward.

74. By engaging in the conduct alleged, Roblox has violated the Stored Communications Act. As a direct and proximate result, Plaintiffs and Class members have suffered the loss of privacy in their stored communications and are entitled to relief as provided by 18 U.S.C. § 2707.

THIRD CAUSE OF ACTION

Violation of the Children's Online Privacy Protection Act (COPPA)

(15 U.S.C. §§ 6502, 6503; 16 C.F.R. Part 312 – Unlawful Collection of Children's Personal Information)

75. Plaintiffs reallege and incorporate all preceding paragraphs as though

fully set forth herein. This cause of action is brought on behalf of the Minor Subclass (children under 13 and their parents/guardians in the Class), with Plaintiffs Michael and Salena Garcia acting in a representative capacity for Plaintiff R.G. and similarly situated minors..

76. **COPPA Overview and Standing**: COPPA is a federal statute designed to protect the privacy of children under 13 years of age online. It applies to operators of commercial websites or online services directed to children, and to operators who have actual knowledge that they are collecting personal information from children under 13. Under COPPA, such operators must provide notice of their data practices and obtain verifiable parental consent before collecting, using, or disclosing personal information from children. COPPA is enforced by the Federal Trade Commission (FTC) and state attorneys general, and does not provide a private damages right of action for individuals. Plaintiffs are not seeking damages under COPPA (which only the FTC/AG can pursue in the form of civil penalties). Instead, Plaintiffs invoke COPPA here to establish Roblox's violations of law as a predicate to equitable relief and to highlight that Roblox's purpose in its interception scheme was illegal (thereby negating any consent defense under ECPA). Plaintiffs seek injunctive and declaratory relief to enforce COPPA's requirements, complementing government enforcement. In essence, Plaintiffs ask this Court to recognize Roblox's conduct as unlawful under COPPA and to order Roblox to come into compliance, even though the Court cannot award COPPA civil penalties to private plaintiffs.

77. **Operator of Child-Oriented Service with Actual Knowledge**: Roblox is unquestionably an "operator" of an online service directed to children, and it also has actual knowledge that children under 13 use its service. Roblox's platform appeals to children through its content and marketing (bright, cartoon-like games, a #1 kids' gaming platform reputation). Roblox even has special account settings for "<13" users, indicating it knows it caters to children. At a minimum, Roblox had

actual knowledge of users' ages because it asks for birth date at account creation. In R.G.'s case, her birth date (supplied at sign-up) showed she was under 13, giving Roblox concrete knowledge of collecting her data as a child. Roblox's own disclosures and external evaluations note that a huge portion of its user base is under 13. Therefore, Roblox falls under COPPA's scope as an operator both directed to children and with actual knowledge of child users.

78. **Personal Information Collected from Children**: COPPA defines "personal information" (PI) broadly at 15 U.S.C. § 6501(8) and in the FTC rules (16 C.F.R. § 312.2). The personal information that Roblox collected from children like R.G. includes, at least:

a. **Persistent Identifiers**: Roblox collected persistent identifiers that can recognize a user over time and across different websites or services (such as cookies, device identifiers, IP addresses, or unique user IDs). These are expressly included in COPPA's definition of PI. Roblox not only collected such IDs (like deviceUniqueID, cookies, IP), but used them for purposes beyond internal operations, including analytics and possibly advertising. COPPA's Rule exempts collection of persistent identifiers without consent only if used solely to support internal operations of the site (e.g., user login, site navigation). Here, Roblox's use of identifiers for cross-site tracking or targeted advertising disqualifies it from the "internal operations" exception. Thus, the persistent identifiers collected from R.G. and other children are regulated personal information under COPPA.

b. **Activity/Profile Information**: By tying persistent IDs to a child's activities (games played, interactions, in-game purchases), Roblox effectively compiled personal information about the child's behavior. Even if certain data points (like a game preference) are not individually listed in COPPA's definition, when linked to a persistent identifier associated with a child, it becomes identifying in context. Roblox's data on a child user's gameplay

habits and friends list becomes part of that child's personal profile.

c. **Children's Provided Information**: If Roblox collected any information directly from children (for example, a child's name or voice chat recording), that would also be personal information. Roblox typically uses usernames, not real names, but COPPA covers any "online contact information" or any information about the child combined with an identifier. Roblox did solicit a parent's email for <13 accounts (for account recovery), which is arguably the parent's PI, but still related to the child's account. Also, any user-generated content from a child that contains personal info (like if a child typed their age or school in a chat, and it slipped through filters and got stored) would be PI. We do not allege specific instances of that for R.G., but note the platform has the capacity to capture such data.

d. **Photos/Recordings**: COPPA also includes photos, videos, and audio recordings of a child as personal info. Roblox introduced features like age verification that involve taking an ID scan and selfie—supposedly not available to under-13 accounts, but children could lie about age to attempt it. If any under-13 users provided a selfie or used voice chat (which involves audio recordings sent to Roblox servers for moderation), those would be additional COPPA-regulated data. We do not rely on this but mention it to illustrate the range of data at issue..

79. In summary, Roblox collected persistent identifiers and associated data from children under 13 (including R.G.) without parental consent. This alone is a COPPA violation. Those identifiers were used to track and target the child's experience, going beyond internal operations, as evidenced by Roblox's own use of data for personalized content and integration of third-party analytics.

80. **Failure to Provide Notice and Obtain Parental Consent**: Roblox failed to comply with COPPA's core requirements: obtaining verifiable parental consent and providing clear notice of information practices. No verifiable parental

consent was ever obtained from Plaintiffs Michael or Salena Garcia (or other parents in the Class) before Roblox collected R.G.'s personal information. The account sign-up for R.G. did not involve any mechanism for a parent to provide consent; it was R.G. herself (a child) who accepted terms. Roblox did not implement any of COPPA's approved methods of obtaining parental consent (such as requiring a signed form, credit card verification, calling a toll-free number, etc.). In fact, Roblox allowed R.G. to create an account and start using the platform with merely a checkbox by the child – a process that blatantly bypasses parental involvement.

81. Roblox also failed to provide direct notice to parents of what information it collects from children, how it uses it, and how parents can consent or refuse, as required by 16 C.F.R. § 312.4. Plaintiff Salena Garcia never received an email or any notification from Roblox informing her that it would collect R.G.'s personal data and asking for her permission. Roblox's privacy policy (even if a parent found and read it) is written in general terms and does not clearly alert a reasonable parent that "we will fingerprint your child's device and track them across the internet." Moreover, COPPA requires a prominent notice of rights and data uses. Roblox's omissions in this regard violated § 312.4's notice provisions.

82. By collecting children's personal information without consent, Roblox violated 15 U.S.C. § 6502(a)(1) which prohibits an operator from collecting personal info from a child in violation of the regulations. The FTC's COPPA Rule provisions that Roblox violated include: 16 C.F.R. § 312.5 (requiring verifiable parental consent) – Roblox did not obtain this; 16 C.F.R. § 312.4 (requiring direct notice to parents) – Roblox failed to provide this; and 16 C.F.R. § 312.3 (general requirement of parental consent for any collection, use, or disclosure of child's personal info) – Roblox violated this by its entire practice. Each child user in the Class represents a repeat COPPA violation (the law treats each child or each day of violation separately for enforcement purposes).

83. **Use and Disclosure of Children's Data (Beyond "Internal Operations")**: COPPA allows an operator to collect certain personal information from a child without parental consent only if it is used solely to support the internal operations of the service (which includes basic functions like authentication, security, maintaining or analyzing the service, or serving contextual ads, etc., but not behavioral targeting or profiling). In Roblox's case, the data collected from kids was used for more than internal support. Roblox leveraged children's persistent IDs to serve personalized ads and content, and it integrated third-party analytics that resulted in disclosing those IDs and related data to outside parties (like Google). For example, sending a child's device fingerprint or ID to Google Analytics is a disclosure of personal info to a third party, which is forbidden without consent. Roblox also likely used children's data to optimize engagement and monetization, which is a business purpose outside the narrow internal operations exemption. Therefore, Roblox cannot claim any safe harbor for what it did with kids' data; its conduct squarely falls under the kind of use COPPA forbids absent parental consent.

84. **Statutory Violations**: By its actions, Roblox violated COPPA's statutory mandate, 15 U.S.C. § 6502(a)(1), which makes it unlawful for an operator of a website or online service directed to children (or with actual knowledge of child use) to collect personal information from a child in a manner that violates the regulations. Roblox's failure to obtain consent and its improper data use violated multiple provisions of the COPPA Rule, including but not limited to 16 C.F.R. § 312.5 (Consent), § 312.4 (Notice), and § 312.3 (general compliance). Each instance of collecting a child's persistent identifier and using it for non-internal purposes without consent is a violation. The class period (from 2021 to present) encompasses repeated, continuous COPPA violations by Roblox affecting potentially millions of children.

85. **Relief Under COPPA (Injunctive and Declaratory)**: While COPPA

does not grant a private right of action for damages, this Court can and should use its equitable powers to enforce compliance with COPPA in order to protect the children in the Class from ongoing and future harm. Plaintiffs seek an injunction requiring Roblox to fully comply with COPPA moving forward. Such an injunction would include, at minimum: (a) ordering Roblox to delete all personal information collected from Class members who were children under 13 at the time of collection, to the extent such data was collected without parental consent; (b) requiring Roblox to implement a verifiable parental consent mechanism for any future collection of personal info from children, should it continue to allow under-13 users (or alternatively, to prohibit children from using Roblox until such a mechanism is in place and verified); (c) requiring Roblox to provide notice to all parents of current users under 13 detailing what information has been collected from their children and how it has been used or shared, and giving those parents an opportunity to provide consent or demand deletion; and (d) enjoining Roblox from using or disclosing any previously collected child data for any purpose unless and until it obtains parental consent, and even then only for permitted purposes. In essence, Roblox should purge the ill-gotten data and not benefit from it.

86. Plaintiffs also seek a declaratory judgment that Roblox's described practices violate COPPA. Such a declaration will serve the public interest by officially documenting Roblox's non-compliance, thereby supporting enforcement by the FTC or state AGs and guiding Roblox's behavior. COPPA further provides that violations are considered unfair or deceptive acts or practices under the FTC Act (15 U.S.C. § 6502(c)). While private parties cannot directly sue under the FTC Act, this finding underscores the gravity of Roblox's misconduct. It bolsters Plaintiffs' argument that injunctive relief is in the public interest to stop an unfair practice targeting children.

87. By vindicating COPPA through this count, Plaintiffs reinforce that Roblox's conduct was not only a private affront but a matter of public concern.

Stopping Roblox's COPPA violations will help ensure a safer environment for children on the platform and align Roblox's operations with the law.

88. (Plaintiffs note that this COPPA count is pleaded to facilitate equitable relief and to highlight the tortious and unlawful purpose behind Defendant's actions. It does not seek duplicative penalties reserved to regulators. Instead, it asks the Court to use its authority to protect the children in the Class and to declare Roblox's duty to comply with the law.)

PRAYER FOR RELIEF

WHEREFORE, plaintiffs, individually, on behalf of the Class and on behalf of the public, pray for judgment as follows:

A. **Class Certification**: An order certifying this case as a class action under Rule 23, appointing Plaintiffs as class representatives for the Class (with Michael and Salena Garcia as representatives of the Adult Subclass and guardians for the Minor Subclass, and R.G. by and through her guardians as representative of the Minor Subclass), and appointing Plaintiffs' attorneys as Class Counsel.

B. **Declaration of Illegality**: A declaration that Defendant Roblox Corporation's actions as alleged herein violate the Electronic Communications Privacy Act (18 U.S.C. § 2510 et seq.), the Stored Communications Act (18 U.S.C. § 2701 et seq.), and the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.), as well as a declaration that Roblox's purported consents or justifications for such conduct are null and void due to its unlawful purpose.

C. **Injunctive Relief**: A permanent injunction prohibiting Roblox, its officers, agents, affiliates, and all persons in active concert with it from engaging in the unlawful practices described. Such injunction shall, among other things, require Roblox to remove or disable any code or functionality in its website and apps that intercepts user communications or tracks users without express consent; to stop injecting third-party trackers or transmitting user data to third parties (like analytics or advertising partners) unless and until users (or parents of minor users) are provided clear notice

and give informed consent; and to implement a robust privacy program that includes age screening and parental consent for any data collection from users known to be under 13. The injunction should further mandate Roblox's compliance with COPPA, including deletion of all personal data collected from children without parental consent, implementation of verifiable parental consent mechanisms going forward, and regular reporting to the Court (or an overseer) on its progress and compliance.

D. **Damages (ECPA)**: An award of statutory damages to Class members under the ECPA, 18 U.S.C. § 2520(c)(2), in the amount of at least $10,000 per Class member, or such greater amount as is proven for those class members whose period of interception warrants a higher award (up to $100 per day per person for each day of violation). The Court has discretion in awarding ECPA damages, and Plaintiffs seek the maximum amount that is just and appropriate for each Class member given the egregious nature of the violations.

E. **Damages (SCA)**: An award of statutory damages to Class members under the SCA, 18 U.S.C. § 2707(c), in the amount of at least $1,000 per Class member (for each violation or per person as the Court deems just). In the alternative, Class members seek actual damages and disgorgement of any profits Roblox obtained from the unauthorized access and disclosure of their communications, to the extent such amount exceeds the statutory minimum.

F. **Punitive Damages**: An award of punitive damages in an amount sufficient to punish Roblox for its willful, reckless, and malicious conduct and to deter such conduct in the future. Given Roblox's size and the scope of wrongdoing, Plaintiffs seek punitive damages to be determined at trial that are proportional to harm and wrongdoing (for example, a multiple of the aggregate statutory damages or an amount otherwise deemed appropriate by the jury and the Court).

G. **Attorneys' Fees and Costs**: An award of reasonable attorneys' fees and litigation costs incurred by Plaintiffs in connection with this action, as authorized by 18 U.S.C. § 2520(b)(3) (ECPA) and 18 U.S.C. § 2707(b)(3) (SCA), and any other applicable

law. Plaintiffs also seek any applicable interest on these amounts.

H. **Restitution/Disgorgement (if applicable)**: To the extent allowed by law, an order of restitution or disgorgement requiring Defendant to return or destroy all ill-gotten data and to disgorge any revenues earned from the exploitation of Class members' data. (For example, any profits attributable to targeted advertising or increased usage resulting from the unlawful tracking should be subject to disgorgement.)

I. **Any Further Relief**: Such other and further relief as the Court deems just and proper, including court-supervised corrective measures or monitoring to ensure Defendant's compliance with the Court's orders.

Jury Trial Demand: Plaintiffs hereby demand a trial by jury on all claims so triable. Plaintiffs request that the issues of their entitlement to damages and the amounts of statutory and punitive damages be determined by a jury at trial.

RESPECTFULLY SUBMITTED

Dated: April 16, 2025

Robert B. Salgado, Esq.
Attorney for Plaintiffs