

1 Robert C. Schubert S.B.N. 62684
2 Willem F. Jonckheer S.B.N. 178748
3 Amber L. Schubert S.B.N. 278696
4 **SCHUBERT JONCKHEER & KOLBE LLP**
5 2001 Union Street, Suite 200
6 San Francisco, CA 94123
7 Tel.: (415) 788-4220
8 Fax: (415) 788-0161
9 rschubert@sjk.law
10 wjonckheer@sjk.law
11 aschubert@sjk.law

12 Christian Levis (*pro hac vice* forthcoming)
13 Amanda Fiorilla (*pro hac vice* forthcoming)
14 Rachel Kesten (*pro hac vice* forthcoming)
15 Yuanchen Lu (*pro hac vice* forthcoming)

16 **LOWEY DANNENBERG, P.C.**
17 44 South Broadway, Suite 1100
18 White Plains, NY 10601
19 Tel.: (914) 997-0500
20 Fax: (914) 997-0035
21 clevis@lowey.com
22 afiorilla@lowey.com
23 rkesten@lowey.com
24 ylu@lowey.com

25 *Attorneys for Plaintiff and the Proposed Class*

26 **UNITED STATES DISTRICT COURT**
27 **NORTHERN DISTRICT OF CALIFORNIA**

28 NICHOLAS RAPAK, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

ADOBE INC.,

Defendant.

Case No. _____

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

1 Plaintiff Nicholas Rapak, individually and on behalf of all other similar situated individuals, asserts
2 the following against Defendant Adobe Inc. (“Adobe”) based upon personal knowledge, information and
3 belief (where applicable), and the investigation of counsel.

4 **SUMMARY OF ALLEGATIONS**

5 1. The internet is not the Wild West. Individuals using the internet have a baseline expectation
6 of privacy, in which they do not expect any company to engage in wide-spread surveillance of all their
7 online activity, especially without affirmative consent.

8 2. Consistent with this expectation, several companies have begun to move away from user-
9 based online tracking in recognition that it is privacy invasive. This began in the early 2010’s, when Apple
10 Inc. announced it would no longer allow companies to collect UDID, which is a permanent device
11 identifier that was used for online advertising. Similar changes followed in the next decade, with the roll
12 out of additional privacy-preserving features like Apple’s “Do Not Track” setting, which sought to limit
13 the collection of advertising IDs from mobile device users, as well as updates by several browsers to
14 block “third-party” cookies (i.e., text files placed on a user’s device from domains they are not visiting),
15 which are used to track users across multiple websites.

16 3. Adobe did the opposite. While other companies moved away from privacy-invasive
17 tracking technology, Adobe sought to capitalize on this shift by building a workaround that would track
18 users regardless of browser, device, or settings. In addition to already-existing identifiers used by Adobe,
19 it launched a new identity solution called the “Experience Cloud Identity Service” just after the
20 deprecation of UDID, followed by the “Experience Platform Identity Service.”

21 4. The **Experience Cloud Identity Service** filled the hole left by the removal of the UDID
22 by Apple. Through this service, Adobe assigns a unique, persistent identifier—set via a first-party
23 cookie—called the Experience Cloud ID (“ECID”) to each website visitor. Companies using Adobe
24 products—such as Adobe Analytics, Adobe Target, or Audience Manager—can deploy the ECID across
25 their digital properties to uniquely identify individual users. Adobe also began assigning the “demdex.net”
26 cookie to all its customers’ unique users—which is closely tied to ECID—so it can track the same user
27 across web properties owned by different organizations.

1 5. Building on ECID and the demdex.net cookie, Adobe then released **Adobe Experience**
2 **Platform Identity Service**. Through this service, Adobe creates an “identity graph” that links “identities
3 together.” For instance, the identity graph will match the ECID to users’ advertising identifiers (e.g.,
4 IDFA/ADID), and even more permanent forms of personally identifiable information, such as email
5 addresses, phone numbers, usernames, and account numbers.

6 6. Adobe combines its Adobe Experience Platform Identity Service with other analytics and
7 marketing products it offers, including **Adobe Real Time Customer Profiles**. These profiles merge
8 multiple unique identifiers together, alongside data reflecting individual’s private interactions and
9 behaviors on the web properties. These profiles include user attributes (e.g., name, age, gender), behavior
10 (e.g., private communications with website owners, such as user searches), audience membership (e.g.,
11 audiences the website owner has placed them in, such as “users who live in California”), and identifiers
12 (e.g., email, phone, device identifiers, and cookies). This additional user data comes from Adobe’s suite
13 of marketing and analytics tracking technology found across the internet, including its Data Collection
14 Tag. Using Adobe Real-Time Customer Profiles, Adobe can enrich the data and uncover even more
15 information about the user, such as actions they are likely to take in the future.

16 7. Adobe’s role as a centralized identity broker allows it to develop complete profiles of
17 individuals and recognize them across websites and devices—exactly what privacy-preserving
18 mechanisms are meant to prevent.

19 8. Adobe leverages the data collected through its Experience Cloud Identity Service—and the
20 consumer profiles it creates—for its own benefit. For instance, Adobe allows customers to use these
21 profiles in Adobe Target. Adobe charges customers to use Adobe Target, which leverages ECID and the
22 Adobe consumer profiles, to create “personalized interactions” and “content” based on the individual’s
23 unique circumstances, such as where they live, what they are interested in, and what actions they have
24 taken previously. Adobe also integrates its Experience Cloud Identity Service with its Audience Manager
25 and Adobe Analytics, which are other ways companies can use these unique user profiles to target the
26 individual user through Adobe.

1 9. Through these identity solutions—and complimentary products—Adobe has been secretly
2 harvesting and monetizing directly identifiable user data from millions of U.S. residents without their
3 knowledge and consent.

4 10. Plaintiff and Class Members had no knowledge that Adobe was using unique, persistent
5 identifiers to track them and their private communications across the internet, or that it was using this data
6 to facilitate targeted advertising.

7 11. Adobe itself does not disclose the extent of its persistent, user-specific tracking, nor does
8 it prompt users viewing the websites or other web properties that use its identifiers of its presence, data
9 collecting, or processes.

10 12. Adobe’s interception of the contents of their communications with third parties through its
11 tracking technology violates Cal. Penal Code § 631, and its installation of a tracking device on each of the
12 websites they use across the internet violates Cal. Penal Code § 638.51(a), as well as other laws.

13 **PARTIES**

14 **A. Plaintiff**

15 13. Plaintiff Nicholas Rapak is a resident of Montgomery County, Pennsylvania.

16 14. Plaintiff Rapak used several online services, including Marriott’s website, which
17 implemented Adobe’s identifiers and tracking software. Plaintiff Rapak visited and logged into Marriott’s
18 website via a web browser multiple times to search for and book Marriott hotels.

19 15. Unbeknownst to Plaintiff Rapak, Adobe assigned him an Adobe Experience Cloud ID
20 (ECID) when he used certain online services, including Marriott’s website.

21 16. Adobe also used other software to track Plaintiff Rapak, including Adobe Audience
22 Manager, Adobe Analytics, and the Adobe Experience Platform script. Through this technology, Adobe
23 intercepted, at least: (1) Plaintiff Rapak’s searches on Marriott’s website; and (2) full-string URLs
24 revealing what Plaintiff Rapak was viewing and interacting with on Marriott’s web properties. Adobe
25 processed this data and stored it on its own servers for its own benefit and monetary gain.

26 17. Plaintiff Rapak did not consent to Adobe intercepting his unique identifiers and other
27 personal data, assigning and using unique identifiers to track him across internet-enabled services and
28 devices, or intercepting and using the contents of his private communications for-profit.

1 **B. Defendant**

2 18. Adobe is a Delaware corporation with its principal place of business located in San Jose,
3 California.

4 19. Adobe knowingly and intentionally developed persistent, unique identifiers to track
5 Plaintiff and Class Members across internet-connected services, despite knowing these types of identifiers
6 were at odds with users' expectation of privacy.

7 20. Adobe knew that its identifiers, and especially Adobe Experience Cloud ID (ECID),
8 circumvented existing privacy protections (like the deprecation of UDID) because it developed this
9 identifier specifically as an alternative to such privacy-preserving mechanisms.

10 21. Adobe offered these services to websites, mobile applications, and other services so that it
11 would have a unique way of tracking Plaintiff and Class Members across devices and platforms.

12 22. Adobe knowingly and intentionally used its identifiers, and data associated with it, to
13 facilitate targeted advertisements for profit.

14 **JURISDICTION AND VENUE**

15 23. Jurisdiction is proper under 28 U.S.C § 1332(d) because: (1) the amount in controversy for
16 the Class exceeds \$5,000,000 exclusive of interest and costs, (2) there are more than 100 putative members
17 of the Class, and (3) Plaintiff and a significant portion of Class Members are citizens of a state different
18 from Adobe.

19 24. This Court has personal jurisdiction over Adobe because its principal place of business is
20 in California. Additionally, this Court has personal jurisdiction over Adobe because a substantial part of
21 the events and conduct giving rise to Plaintiff's claims occurred in California, including Adobe's
22 interception and use of Plaintiff's unique identifiers and other personal data.

23 25. Venue is proper under 28 U.S.C. §1391(b), (c), and (d) because a substantial portion of the
24 conduct described in this Class Action Complaint was carried out in this District. Furthermore, Adobe is
25 headquartered in this District and subject to personal jurisdiction in this District.

26 26. This action arises in Santa Clara County, in that a substantial part of the events which gave
27 rise to the claims asserted herein occurred in Santa Clara County. Pursuant to L.R. 3-2(e), all actions that
28 arise in Santa Clara County shall be assigned to the San Jose Division.

1 **BACKGROUND OF USER TRACKING**

2 27. Over a decade ago, Apple announced it would no longer allow app developers to intercept
3 “UDIDs” which are unique, device-specific identifiers. These persistent identifiers were deprecated
4 because they are seen as privacy intrusive—they cannot be reset and were used to facilitate device-specific
5 targeted advertising.

6 28. This trend only continued. Starting in 2020, Apple and Google announced the eventual
7 deprecation of advertising identifiers (IDFA and ADID) and third-party cookies in favor of more privacy-
8 preserving mechanisms.

9 29. The loss of some of the most common unique identifiers raised serious concerns within the
10 multi-billion-dollar digital advertising industry. Digital advertisers relied on these identifiers and cookies
11 to uniquely identify individuals who use their products and services—and other entities’ products and
12 services—to serve targeted advertisements to individuals, based on profiles of information reflecting web
13 and app activity indexed to unique identifiers present in third-party cookies.

14 30. For instance, a mobile app developer would use identifiers like the IDFA and ADID created
15 by iOS and Android phones to track user activity across their mobile application, understand what actions
16 users took and their preferences, interests, and other information. The company would then send that
17 information to an advertising company, such as Google, to serve targeted advertisements to that customer
18 using this unique identifier.

19 31. Proposed solutions to make up for these unique identifiers and third-party cookies were not
20 nearly as effective. For instance, some companies sought to track user “sessions” (i.e., one interaction with
21 the webpage until the user closes out) in lieu of other unique identifiers. However, this alternative was not
22 nearly as powerful as directly tracking an individual at the user or device-level.

23 **ADOBE’S UNIQUE IDENTIFIERS**

24 32. Adobe itself was well aware that there was a “rise in cookie regulation” as reflected in their
25 own marketing materials.

FIGURE 1

33. Rather than embrace these changes, Adobe planned to capitalize on the move away from device identifiers and third-party cookies by Apple and Google by creating a persistent unique, cross-platform identifier of its own.

34. The first identity solution was called Adobe Analytics ID, which it now refers to as its legacy ID. This unique identifier is observable in network traffic as a cookie called `s_vi`. It is often stored as a first-party cookie and used to track a user across a single domain.

35. Adobe went on to develop **Adobe Experience Cloud Identity Service**, which introduced the Adobe Experience Cloud ID (ECID), also known as "MID." The ECID is a first-party cookie that assigns a persistent, unique identifier to each user and enables tracking across Adobe Experience Cloud products, including Analytics, Target, and Audience Manager. Through ECID, Adobe facilitates unified data collection and personalization consistently across their applications.

36. Thus, if a website domain owns two separate web properties, for instance, a hospital patient portal that uses Adobe Analytics and a public-facing website that uses Adobe Target, the same ECID will be assigned to the same user, even though they are different Adobe services. The ECID is stored in the field `s_ecid` and/or in an AMCV cookie. It can also be passed in parameters through network traffic. A single ECID cookie does not expire for two full years.

37. Adobe, however, also uses the ECID framework to track unique users across websites and online services owned by *different* companies. When a company initially sets the ECID, they call Adobe's "Data Collection Server" ("DCS") known as "dpm.demdex.net" and transmit their "organization ID."

1 Adobe’s DCS processes this information and transmits back the user’s ECID (identified in the Figure
 2 below as “MID”) as well as a **demdex.net** cookie. This process is reflected in **Figure 2**, below.

3 **FIGURE 2¹**

4 ID Request



11 ID Response

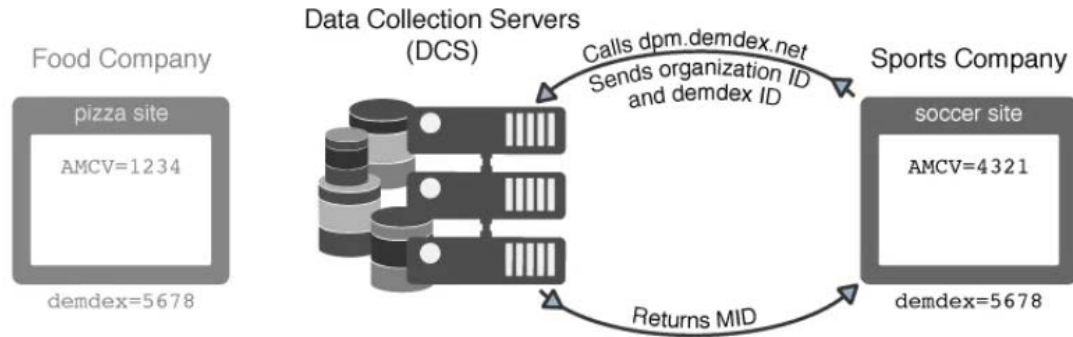


20 38. In the above example, the demdex.net cookie set for the unique visitor who stopped at
 21 “Food Company” is 5678. Because the demdex.net cookie is persistent across websites—even those
 22 owned and operated by different website providers—when the “Food Company” user visits a new website,
 23 the demdex.net cookie continues to track them. This is reflected in **Figure 3**.

24
25
26
27 ¹ *Identity Service Guide*, ADOBE, INC., [https://experienceleague.adobe.com/en/docs/id-](https://experienceleague.adobe.com/en/docs/id-service/using/intro/id-request#concept-2caacebb1d244402816760e9b8bcef6a)
 28 [service/using/intro/id-request#concept-2caacebb1d244402816760e9b8bcef6a](https://experienceleague.adobe.com/en/docs/id-service/using/intro/id-request#concept-2caacebb1d244402816760e9b8bcef6a) (last visited April 2, 2025).

FIGURE 3²

Visitor ID Request & Response



39. As shown in **Figure 3**, when the previous “Food Company” customer visits “Sports Company” Adobe’s DCS assigns the same demdex.net cookie—5678. Thus, Adobe knows the same unique individual who visited “Food Company” is the same unique individual who visited “Sports Company.”

40. If that were not enough, Adobe also assigned other unique identifiers. For instance, if there are “third-party cookie restrictions” Adobe sets a “fallback unique visitor ID” recognized as “s_fid” in network traffic, as well as “s.visitorID” which is another “unique identifier for the visitor.” Adobe also collects IP address.

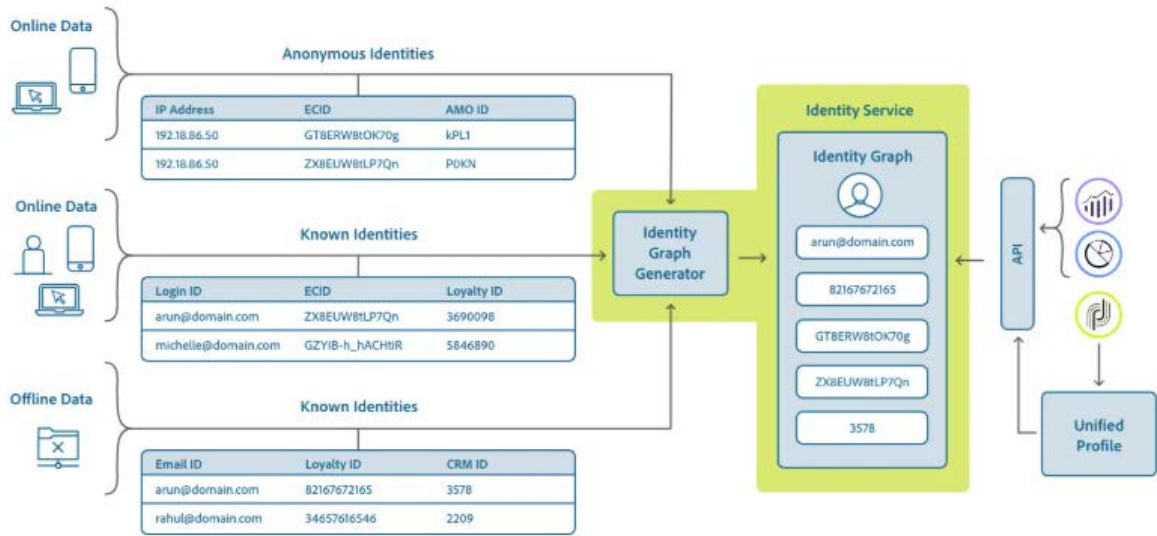
ADOBE’S COMPREHENSIVE IDENTITY SOLUTION

41. Adobe does not just provide identity solutions; it also launched the **Adobe Experience Platform Identity Service** to use these identifiers (and others) to profile users.

42. The Adobe Experience Platform Identity Service is designed to keep identity tracking consistent when the same user logs in or interacts with a website from multiple devices, such as from their phone and then their laptop, which would otherwise create multiple, disparate identifiers. Through this service, Adobe collects all the identifiers across devices and websites and links that to an “identity graph” through what it calls its “Identity Graph Generator.” This associates all the known identifiers with the same individual, even though they would previously appear as multiple unique users.

² *Id.*

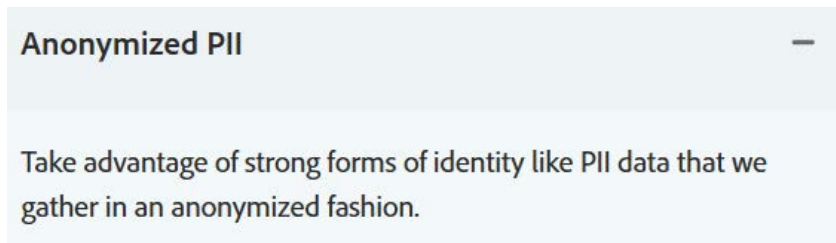
FIGURE 4³



43. As shown in **Figure 4**, through the Adobe Experience Platform Identity Service, Adobe receives identifiers, such as ECIDs, IP address, Login IDs, and email addresses, which it can then reconcile as the same user through its Identity Graph Generator.

44. Adobe incredibly bills its identity solution as gathering “PII data” in an “anonymized fashion.” But both cannot be true at the same time. “Strong forms of identity” like PII data is exactly the opposite of anonymized data.

FIGURE 5⁴



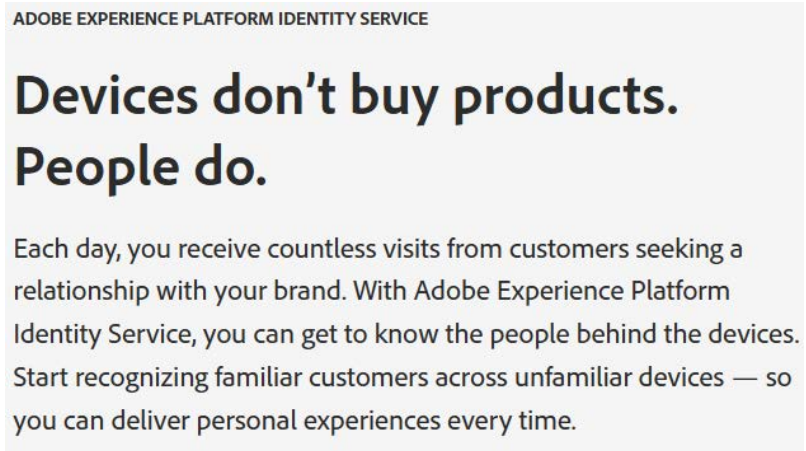
45. Despite its characterization, Adobe knew that this solution was *better* at tracking individuals than previous identifiers, including those being deprecated, and was not anonymized. Indeed, Adobe actively markets its identity solution as unique because it identifies the specific “*people behind the*

³ Platform Identity Service Guide, ADOBE, INC., <https://experienceleague.adobe.com/en/docs/experience-platform/identity/home> (last visited April 2, 2025).

⁴ Experience Platform Identity Service, ADOBE INC., <https://business.adobe.com/products/experience-platform/identity-service.html> (last visited Apr. 1, 2025).

1 *devices*”—not just devices.

2 **FIGURE 6⁵**

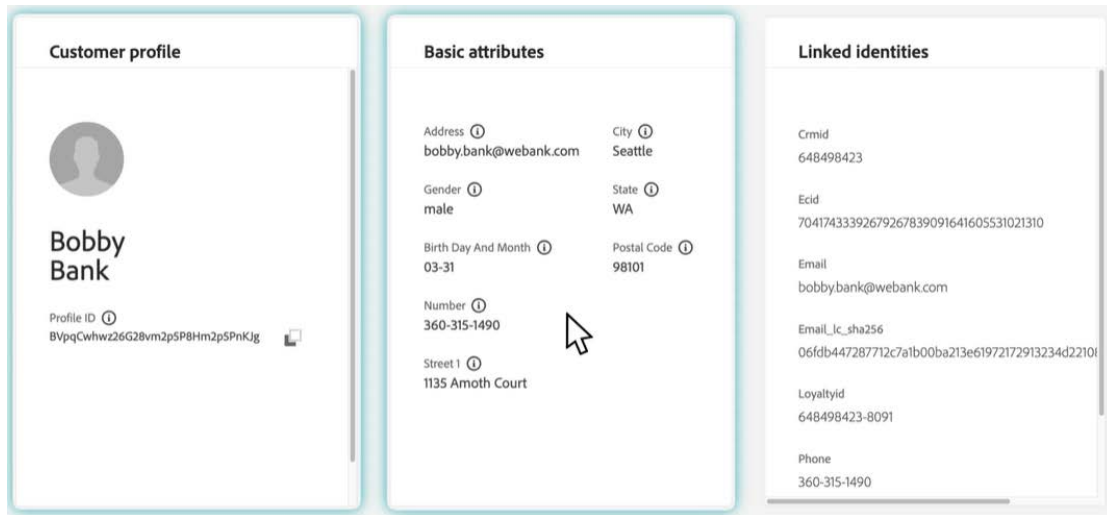


11 46. As shown in **Figure 6**, Adobe itself does not see its identity solutions as either a “session”

12 or “device” level identifier, but a way to identify actual people, akin to a social media profile. **Figure 7**

13 depicts what this profile looks like in the Adobe dashboard.

14 **FIGURE 7**



23 47. In fact, Adobe’s identity solutions are *stronger* identifiers than those that previously

24 existed, as Adobe itself acknowledges. For instance, most first-party cookies are limited in that they only

25 track a user on one specific website. Adobe’s Experience Platform Identity Service goes much further, by

26 tracking users across permanent identifiers, such as email address and IP address, and first-party cookies

27 like ECID. This makes it possible to create an identity profile that serves advertisers’ needs, by aggregating

28 ⁵ *Id.*

1 data across all apps and websites a person uses that incorporates Adobe’s technology, at the expense of
2 individual’s right to privacy.

3 48. Adobe’s status as an identity broker allows it to track users across the internet and develop
4 unique profiles, which Adobe then offers to its customers to use with Adobe’s other marketing and
5 analytics products at a price premium.

6 ADOBE’S EXPERIENCE CLOUD PLATFORM

7 49. Adobe created the Experience Platform Identity Service precisely because of its synergy
8 with its existing (and pricey) analytics, advertising, and AI products. Collectively, all of these services are
9 referred to as the **Adobe Experience Cloud Platform**. A subset of the services included in the Adobe
10 Experience Cloud Platform are described below.

11 50. One of the products Adobe offers is **Adobe Analytics**, which includes its Data Collection
12 Tag. This Adobe Data Collection Tag is deployed directly on web pages and mobile applications. When
13 used, the Data Collection Tag automatically captures the ECID, along with other data and identifiers,
14 including browser type, device characteristics, and IP address. It also collects more sensitive data revealing
15 the user’s communications with the website provider, including pages they visited, searches they
16 conducted, and more. This information is transmitted directly to Adobe’s own servers, as indicated by
17 Adobe owned domains like demdex.net and adobedc.net.

18 51. The Adobe Data Collection Tag intercepts the Adobe Experience Cloud ID (ECID) and
19 online users’ private communications directly from webpages and redirects it to its own servers,
20 aggregating that information with a user’s profile, so it can be used for advertisements, including the
21 creation of custom audiences, lookalike audiences, and campaign optimization.

22 52. The data collected through the Adobe Data Collection Tag is used for developing complex
23 analytics, which reveal more information about the user than the data itself. For instance, Adobe offers
24 **Predictive Analytics** (powered by Adobe Sensei), which it bills as “[p]redicting the future” i.e., future
25 actions likely to be taken by the unique users whose data Adobe intercepted. As Adobe explains, “[h]idden
26 in [the] data” are “patterns” that reveal additional “meaningful insights” that can be “used effectively”
27 (through Adobe, of course) to have a “very real impact on the bottom line.” Adobe provides predictive
28

1 analytics by running the intercepted data through “machine learning and advanced statistical models” to
2 “dig automatically through [the] enormous amounts of data” and uncover new “insights” about the user.

3 53. **Adobe Audience Manager** is yet another product in the Adobe Experience Cloud Platform
4 that works with Adobe Analytics and the Adobe Experience Platform Identity Service. In Adobe Audience
5 Manager, Adobe customers can use its “proprietary algorithm” called “TraitWeight” to discover “new,
6 unique audience members.” The Adobe customer selects users and “trait[s]” or “segment[s]” associated
7 with them—as identified through Adobe Analytics and the Adobe Experience Platform Identity Service—
8 and then sends Adobe’s algorithm to search the existing database for individuals likely to take similar
9 actions as the originally selected individuals. Adobe’s algorithm provides a “weighted score” reflected
10 how similar the newly identifiers users are to the ones initially selected. Adobe Analytics can send data to
11 Adobe Audience Manager in real-time through server-side forwarding.

12 54. **Adobe Campaign** similarly integrates with Adobe Analytics and the Adobe Experience
13 Platform Identity Service. Adobe allows customers to use their “Analytics data directly in [Adobe]
14 Campaign” with customer’s other “email engagement data.” Used together, Adobe customers can use
15 audiences created in Adobe Analytics to send “personalized messages” based on “actions” they have taken
16 on a website. Using “AI” Adobe Campaign can discern and “predict the best send times” that are the “most
17 likely” to get customers to “engage.”

18 55. Likewise, **Adobe Marketo Engage** also syncs with Adobe Analytics and the Adobe
19 Experience Platform Identity Service. Adobe Marketo Engage tracks data like lead details, including users
20 who completed forms, viewed certain pages, or engaged in email interactions. This data is synced through
21 the Adobe Experience Platform Identity Service with data from Adobe Analytics in a unified profile.
22 Adobe Analytics then enriches the Marketo Engage data to create lead scores and generate follow-up
23 content to convert the lead to a customer or achieve some other marketing goal (i.e., converting to a paid
24 customer, start trial, etc.).

25 56. **Adobe Journey Optimizer** is yet another product that can be integrated with Adobe
26 Analytics and the Adobe Experience Platform Identity Service. Adobe Journey Optimizer allows
27 customers to track user’s interactions on a web property, and trigger certain responses based on the actions
28 they take. For instance, if a user adds an item to cart, but does not purchase it, Adobe Journey Optimizer

1 flags this interaction and can be used to create the “perfect offer” to get the user to “engage” and “convert”
 2 by developing “targeted content.” Adobe’s AI can develop the targeted content directly for the Adobe
 3 customer.

4 57. Finally, **Adobe Advertising** also integrates with Adobe Analytics and the Adobe
 5 Experience Platform Identity Service. Combining Adobe Analytics with Adobe Advertising and Adobe
 6 Experience Platform Identity Service enables customers to perform remarketing, measure ad performance,
 7 and engage in campaign optimization based on unique user profiles compiled by Adobe. Adobe
 8 Advertising customers can use these profiles to buy, manage, and optimize advertisements directly through
 9 Adobe, which acts as a Demand-Side Platform for real-time bidding auctions. Adobe encourages
 10 customers to integrate Adobe Advertising with its other products precisely to provide this hyper-specific
 11 type of targeting and ad bidding.

Adobe Product	Integrates with Adobe Analytics	Integrates with Adobe Identity Solution
Adobe Audience Manager	✓	✓
Adobe Campaign	✓	✓
Adobe Marketo Engage	✓	✓
Adobe Journey Optimizer	✓	✓
Adobe Advertising	✓	✓

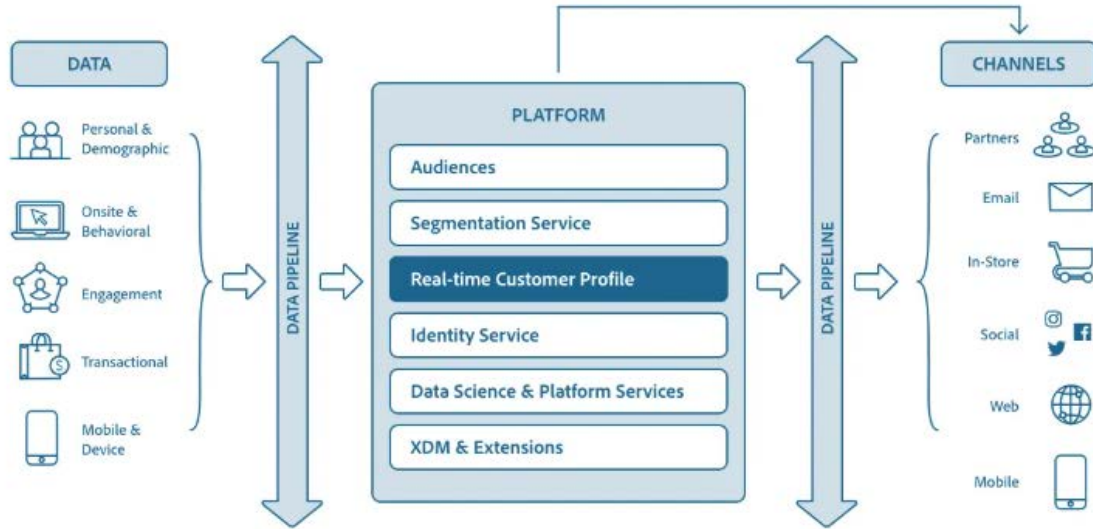
12
 13
 14
 15
 16
 17
 18 **ADOBE’S UNIQUE & COMPREHENSIVE USER PROFILES**

19 58. Adobe offers a clear and easy way to combine the power of most of its marketing and
 20 analytics tools (including Adobe Analytics and Adobe Advertising) with the Adobe Experience Platform
 21 Identity Service all in one place. This is known as **Adobe Real-Time CDP**.

22 59. The Adobe Real-Time CDP ingests data from multiple sources (e.g., Adobe Analytics,
 23 offline data, and other integrated sources), and then uses the Adobe Experience Platform Identity Service
 24 to stitch this data into a comprehensive profile, tracking *both* identity and user’s unique (and private)
 25 interactions. **Figure 8** explains how Real-Time Customer Profiles are used with Adobe’s other services.
 26
 27
 28

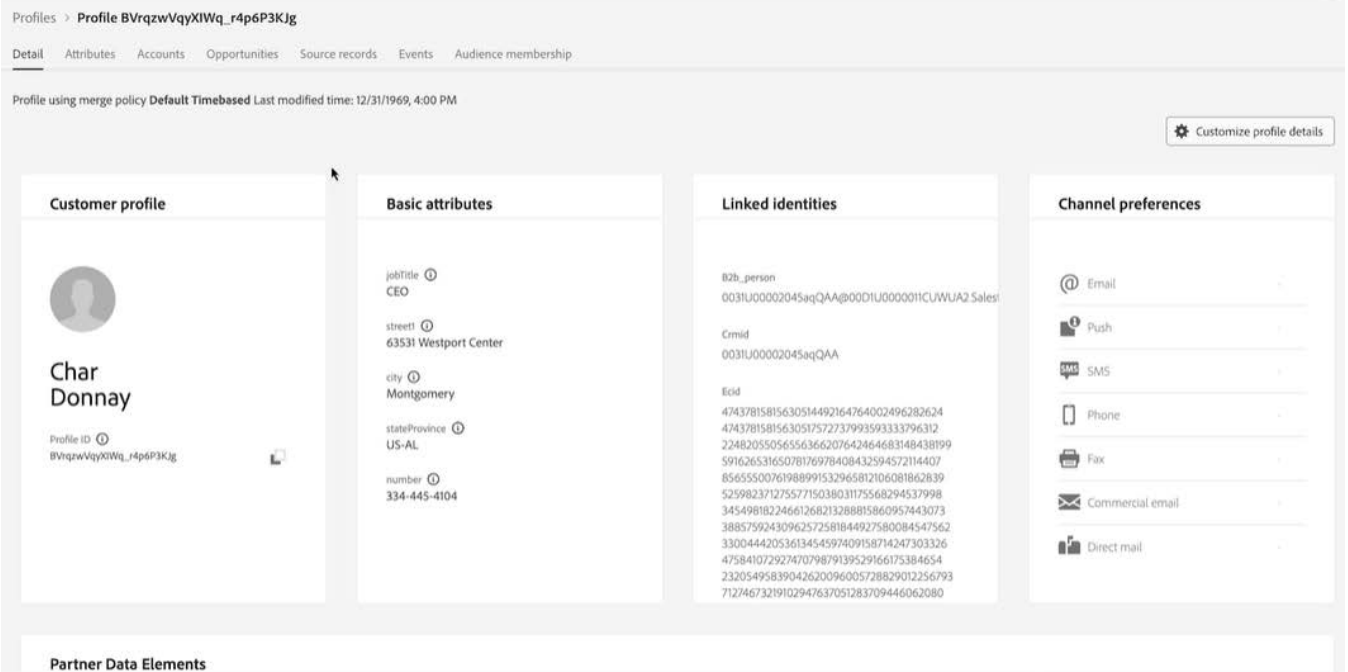
FIGURE 8⁶

Adobe Experience Platform: Core Components



60. What this Adobe-Real Time Customer Profile looks like is depicted in **Figure 9**.

FIGURE 9⁷



⁶ *Real-Time Customer Profile Guide*, ADOBE, INC., <https://experienceleague.adobe.com/en/docs/experience-platform/profile/home> (last visited April 2, 2025).

⁷ *Create and Enhance Customer Profiles*, ADOBE, INC., <https://business.adobe.com/products/real-time-customer-data-platform/create-enhance-customer-profiles.html#marquee> (last visited April 2, 2025).

1 example, showing the user moved from search results to calendar view for hotel prices); (3) the present
2 full-string URL (for instance, indicating the user is viewing the “Rate[]Calendar” for a property with the
3 ID code for the property selected, such as MIATX (i.e., Miami Airport Marriott); and (4) the Company
4 ID (indicating the entity being communicated with is Marriott).

5 68. This is just one example. Thousands of other websites also incorporate services
6 encompassed within the Adobe Experience Cloud Platform.

7 69. For instance, when an individual visits Cedars-Sinai’s website, this also triggers the Adobe
8 Experience Platform Launch script. Like above, this can be observed through developer tools, which
9 indicates the script is triggering a request to “assets.adobem.com.”

10 70. If a user navigates to Cedar-Sinai’s primary care page and then proceeds to the online
11 scheduling page, this information is intercepted by Adobe based on a review of the network traffic. Adobe
12 receives: (1) ECID; (2) the previous full-string URL the user visited (www.cedars-sinai-
13 org/programs/primary-care.html); (3) the present full-string URL (www.cedars-
14 sinai.org/programs/primary-care/digital-scheduling.html); (4) that the user is engaging in online schedule
15 (as indicated by “hasOnlineScheduling:true”); (5) the Adobe Org ID (indicating the data comes from
16 Cedar Sinai); and (6) the Company ID (relaying the same as Adobe Org ID).

17 71. This data is sent to Adobe Edge Network, which is used by Adobe’s Customer Journey
18 Analytics (CJA), Adobe Real-Time CDP, Adobe Journey Optimizer, and Adobe Target. These destinations
19 suggests that Cedars-Sinai compiles this data in, at least, Adobe Real-Time Customer Profiles (described
20 above). Indeed, Adobe automatically promotes customers using Adobe Experience Platform Edge
21 Network to send and merge the data with Real-Time Customer Profiles.

22 72. Separately, users who visit Cedars-Sinai trigger “AppMeasurement.min.js” which
23 indicates that Cedars-Sinai is also an Adobe Analytics customer using its traditional integration. This script
24 also enables sending data directly to Adobe Analytics.

25 **PLAINTIFF AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY**

26 73. Internet users do not expect to be tracked across every single one of their internet-connected
27 devices, including their web browser, apps, TVs, and more.

28

1 74. Indeed, the advent of privacy-preserving mechanisms like Apple’s “Do Not Track” feature,
2 which can prevent companies from collecting IDFA/ADID from individuals who opt-out, and similar
3 features described above, have confirmed this expectation.

4 75. One study by Flurry Analytics in 2021 shows that 88% of iOS users worldwide have
5 availed themselves of this feature, indicating an intent to prevent apps from tracking them on their mobile
6 devices.

7 76. Users do not know—and did not expect—that Adobe would circumvent these protections
8 by creating a new identifier that is even better than IDFA/ADID at tracking them across services.

9 77. Adobe itself does not provide any information for Plaintiff and Class Members to
10 understand which websites or online services use ECID or any of Adobe’s other privacy-offending
11 products, such that they have no way of uncovering which services do or do not contain Adobe’s tracking
12 technology.

13 78. Plaintiff and Class Members reasonably expect that their online activity would not be
14 tracked by an unknown company, let alone that it would be used to target them across online services for
15 profit.

16 79. Adobe did not have consent to perform this type of omni-present cross-device tracking
17 using Plaintiff’s and Class Members’ unique identifiers and private communications.

18 **ADOBE’S CONDUCT VIOLATES ESTABLISHED DATA PRIVACY REGIMES**

19 80. The GDPR and CCPA both mirror Fair Information Practice Principles (FIPPs). Two of the
20 core tenants of FIPPs are (1) clear user consent; and (2) data minimization.

21 81. Adobe does neither of these things. Despite creating a cross-device persistent user
22 identifier, Adobe makes zero effort to ensure Plaintiff and Class Members are even aware of where this
23 technology is used. This is clear from its own Privacy Policy, which makes no attempt to identify the
24 entities using its services.

25 82. Separately, the creation of an ever-present persistent identifier is directly at odds with the
26 idea of data minimization, which requires that data should be stored and used only for the period of time
27 in which that data is necessary. Indeed, the fact that device and user-specific identifiers are persistent (and
28 not deleted) is exactly why even device identifiers like IDFA are being phased out by companies like

1 Apple to preserve users' privacy. Adobe's creation of a maximized identity profile—linking all existing
2 identifiers together—is a regression from today's privacy norms.

3 **TOLLING & CONCEALMENT**

4 83. The earliest Plaintiff and Class Members could have discovered Adobe's conduct was
5 shortly before the filing of this Complaint. Plaintiff became aware of Adobe conduct through
6 communications with counsel that are protected from disclosure.

7 84. Plaintiff and Class Members, despite their due diligence, could not have discovered
8 Adobe's conduct by virtue of how its technology works and its lack of disclosures.

9 85. Adobe's interception of unique identifiers, including ECID, and other personal data and
10 other identifiers happens inconspicuously in the background. This process is undetectable to an ordinary
11 person, highly technical, and prevented Plaintiff and any Class Member from uncovering it.

12 86. Adobe had exclusive knowledge that ECID, its other identifiers, and its tracking
13 technology were tracking Plaintiff and Class Members across the internet alongside their private
14 communications on third-party apps, websites, and other services. Similarly, Adobe had exclusive
15 knowledge that it was using this information to propagate one of the largest targeted advertising systems.

16 87. Adobe's fraudulent conduct prevented Plaintiff and Class Members from discovering its
17 conduct. Adobe maintained a privacy policy that lacked adequate disclosures for Plaintiff and Class
18 Members to uncover that Adobe even intercepted, had, or used their data. Adobe publicly held out its
19 identifiers and technology as privacy-preserving mechanisms, even though they were not.

20 88. Adobe was under a duty to disclose the nature and significance of its data interception and
21 use practices—especially in light of its public statements—but did not do so. Adobe is therefore estopped
22 from relying on any statute of limitations by virtue of the discovery rule and doctrine of fraudulent
23 concealment.

24 **CLASS ACTION ALLEGATIONS**

25 89. Plaintiff brings this action under Fed. R. Civ. P. 23 individually and on behalf of the
26 following Classes:

27 **Identifier Class:** All natural persons in the United States for whom Adobe intercepted
28 or stored an ECID, demdex cookie, or other identifying information, or for whom
Adobe created an Identity Graph.

1 **Communications Class:** All natural persons in the United States who had their
2 communications with third parties intercepted or used by Adobe without their consent.

3 90. The Classes exclude: (1) any judge presiding over this action or their immediate families;
4 (2) Adobe, its subsidiaries, affiliates, parents, successors, predecessors, and any other entity in which
5 Adobe has a controlling interest; (3) Adobe’s current and former employees, officers, and directors; and
6 (4) Plaintiff’s and Adobe’s counsel.

7 91. **Numerosity.** While the precise size of the Classes are currently unknown to Plaintiff, each
8 of the Classes consists of well over a million individuals and members of each of the Classes can be
9 identified through Adobe’s records.

10 92. **Predominant Common Questions.** The Classes’ claims present several common questions
11 of law and fact that predominant over questions (if any) that affect individual class members. This
12 includes:

- 13 a. Whether Adobe violated Plaintiff’s and the Classes’ privacy rights;
- 14 b. Whether Adobe engaged in unfair and deceptive conduct;
- 15 c. Whether Adobe’s acts and practices violate the California Invasion of Privacy Act;
- 16 d. Whether Plaintiff and Class Members are entitled to damages and/or equitable relief,
17 including injunctive relief, restitution, and disgorgement; and
- 18 e. Whether Adobe was unjustly enriched.

19 93. **Typicality.** Plaintiff’s claims are typical of all Class Members because they arise from the
20 same conduct and are based on the same legal theories.

21 94. **Adequate Representation.** Plaintiff will (and has) fairly and adequately represented the
22 Classes and protected the interest of all Class Members. Plaintiff has retained competent counsel with
23 significant experience in class action and data privacy litigation. Plaintiff and counsel have no interest that
24 conflicts with the interests of the Classes and is not subject to any unique defenses. Plaintiff and their
25 counsel will vigorously prosecute this action to advance the interest of the Classes and have the resources
26 necessary to do so.

27 95. **Substantial Benefits.** A class action is superior to all other possible methods to fairly and
28 efficiently adjudicate this case and controversy, and joinder of all Class Members is impracticable.

1 Proceeding as a class case has significant advantages to individual litigation, including: (1) comprehensive
2 oversight by a single court, which avoids inconsistent outcomes; and (2) saving time and expense by
3 litigating the same claims arising from the same conduct all in one action.

4 96. Plaintiff reserves all rights to revise or modify the class allegations based on facts and legal
5 developments following additional investigation or discovery.

6 **CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS**

7 97. California law applies to every Class Member’s claims. Adobe maintains its principal place
8 of business in California and conducts substantial business in California, including the activities giving
9 rise to Plaintiff’s and Class Members’ claims. Adobe’s decision to reside in California and avail itself of
10 California’s laws makes the application of California law to its conduct alleged herein constitutionally
11 permissible. Adobe also elects to apply California law in its Terms of Use and Privacy Policy.

12 98. Under California’s choice of law rules, the application of California law is appropriate
13 because California has significant contacts to the claims and Parties in this action, California has a greater
14 interest in applying its laws, given Adobe’s residency in the State and the location of the conduct at issue,
15 over any other state.

16 **CLAIMS FOR RELIEF**

17 **FIRST CAUSE OF ACTION**

18 **Violation of Common Law Invasion of Privacy (Intrusion Upon Seclusion)
19 On Behalf of the Plaintiff and Classes**

20 99. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
21 same force and effect as if fully restated herein.

22 100. Intrusion upon seclusion requires pleading: (1) that the defendant intruded on a place,
23 conversation, or matter in which Plaintiff has a reasonable expectation of privacy; and (2) that the intrusion
24 would be highly offensive to a reasonable person.

25 101. Adobe’s collection, interception, and use of Plaintiff’s and Class Members’ personally
26 identifiable information constitutes an intentional intrusion. As does its use of this information to create
27 “identity graphs,” the latter of which is based off these identifiers to track and profile Plaintiff and Class
28 Members based on their online activity.

1 102. Adobe’s interception and use of Plaintiff’s and Class Members’ private online
2 communications, associated with their assigned ECID and other identifying information, is likewise an
3 intentional intrusion upon Plaintiff’s and Class Members’ solitude.

4 103. Plaintiff and Class Members reasonably expected their unique identifiers and other
5 personal data, alongside their online activity, would not be intercepted or used by an unknown third-party.
6 The types of identifying information Adobe stored in “identity graphs” are particularly private because
7 they are often directly identifiable, permanent identifiers (e.g., IP address, phone number, email). Plaintiff
8 and Class Members reasonable expected this information would remain private and confidential and
9 would not be intercepted or used by third parties without their consent.

10 104. This expectation is particularly heightened given that there were no disclosures of Adobe’s
11 involvement in intercepting, processing, and using their unique identifiers and other personal data and
12 online communications.

13 105. Plaintiff and Class Members did not consent to, authorize, or understand Adobe’s
14 interception or use of their private data.

15 106. Adobe’s conduct is highly offensive because it violates established social norms.
16 Consumers do not expect to be surveilled whenever they use the internet, especially in light of state laws
17 requiring companies to make adequate disclosures regarding their collection and use of data.

18 107. Adobe’s conduct is particularly offensive in light of the secretive nature in which it takes
19 place. Plaintiff and Class Members had no way of knowing Adobe collected their unique identifiers and
20 other personal data and other online communications, and Adobe did so from thousands of websites, if
21 not more.

22 108. Adobe’s conduct caused Plaintiff and Class Members harm and injury, including a violation
23 of their privacy interests.

24 109. Plaintiff and Class Members seek damages to compensate the harm to their privacy
25 interests, among other damages, as well as disgorgement of profits made by Adobe as a result of its
26 intrusion upon seclusion.

1 110. Defendant’s conduct was willful, knowing, and carried out with a conscious disregard for
2 Plaintiff’s or Class Members’ rights, Plaintiff’s and Class Members are entitled to punitive and exemplary
3 damages.

4 111. Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

5 **SECOND CAUSE OF ACTION**

6 **Violation of Article I, Section 1 of the California Constitution (Invasion of Privacy)**
7 **On Behalf of the Plaintiff and Classes**

8 112. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
9 same force and effect as if fully restated herein.

10 113. Article I, Section 1 of the California Constitution provides: “All people are by nature free
11 and independent and have inalienable rights. Among these are enjoying and defending life and liberty,
12 acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”
13 California Constitution, Article I, Section 1.

14 114. To state a claim for invasion of privacy under the California Constitution, a plaintiff must
15 establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an
16 intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of
17 the social norms.

18 115. The right to privacy in California’s Constitution creates a right of action against private
19 and government entities.

20 116. Plaintiff and Class Members have and continue to have a reasonable expectation of privacy
21 in their personal information, identities, and private data, pursuant to Article I, Section I of the California
22 Constitution.

23 117. The identifiable and private information Adobe intercepted, stored, and used without
24 Plaintiff’s and Class Members’ consent was used to track them consistently, and persistently, across
25 internet-connected services and to serve targeted advertisements. The manner in which Adobe intercepted
26 this information defeated established privacy-mechanisms and social norms.

27 118. This conduct constitutes an extremely serious invasion of privacy that would be highly
28 offensive to a reasonable person. Reasonable individuals do not expect that there is an entity intercepting
and monitoring all of their online activity, let alone using it for profit.

1 119. Adobe’s conduct violated the privacy of hundreds of thousands (if not millions) of Class
2 Members, including Plaintiff. Adobe did not have consent to intercept this information, let alone use it.

3 120. Plaintiff and Class Members seek damages to compensate the harm to their privacy
4 interests, among other damages, as well as disgorgement of profits made by Adobe as a result of its
5 intrusion upon seclusion.

6 121. Defendant’s conduct was willful, knowing, and carried out with a conscious disregard for
7 Plaintiff’s or Class Members’ rights, Plaintiff and Class Members are entitled to punitive and exemplary
8 damages.

9 122. Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

10 **THIRD CAUSE OF ACTION**
11 **Violation of the California Invasion of Privacy Act (“CIPA”)**
12 **Cal. Penal Code § 631**
13 **On Behalf of the Plaintiff and Classes**

14 123. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
15 same force and effect as if fully restated herein.

16 124. CIPA § 631 prohibits any person who by means of any “machine, instrument, contrivance”
17 or in “any other manner:” (1) intentionally taps or makes an unauthorized connection with “any telegraph
18 or telephone wire, line, cable, or instrument;” (2) willfully and without consent of “all parties to the
19 communication” or in “any unauthorized manner” reads or “attempts to read” or “learns the contents or
20 meaning of any message, report, or communication while the same is in transit or passing over any wire,
21 line, or cable, or is being sent from, or received at any place within” California; (3) “uses, or attempts to
22 use, in any manner, or for any purpose, or to communicate in any way” information so obtained; or (4)
23 from aiding, agreeing, employing, or conspiring with “any person or persons to unlawfully do, or permit,
24 or cause to be done any of the acts or things mentioned above in this section.”

25 125. Adobe is a person under CIPA § 631.

26 126. Adobe maintains its principal place of business in California, which is where it designed,
27 created, conspired, and effectuated the interception and use of Plaintiff’s and Class Members’ unique
28 identifiers and other personal data and private communications.

1 127. Adobe’s technology (e.g., the Adobe Data Collection Tag, Adobe Experience Cloud ID
2 (ECID) framework, etc.), and Plaintiff’s and Class Members’ computers, mobile devices, and connected
3 TVs, are each a “machine, instrument, contrivance, or . . . other manner” under CIPA § 631.

4 128. At all relevant times, Adobe used its technology to make unauthorized connections with
5 the lines of communication and instruments used by Plaintiff and Class Members to access online services
6 without the consent of all parties to those communications.

7 129. Adobe willfully, and without consent, read or attempted to read, or learn the contents and
8 meaning of, Plaintiff’s and Class Members’ communications with online services while those
9 communications were in transmit or passing over a wire, line, or cable, or were being sent or received
10 within California through its tracking technology, as described herein. This interception happens prior to
11 or at the same time they would be received by the intended recipient.

12 130. Adobe used, and attempted to use, these identifiable, private communications for its own
13 benefit, including targeted advertising as described herein.

14 131. Adobe also aided, agreed with, employed, and conspired with website operators and
15 advertising entities to intercept and use this data for profit.

16 132. The interception and use of Plaintiff’s and Class Members’ communications was without
17 authorization or consent from Plaintiff and Class Members.

18 133. Plaintiff and Class Members have been harmed as a result of Adobe’s conduct. Their
19 private data has been intercepted, viewed, and used for targeted advertising and has not been destroyed.
20 Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored
21 and used, such that Plaintiff and Class Members have no adequate remedy at law.

22 134. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a), which
23 provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of damages sustained
24 by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable
25 relief.

26 **FOURTH CAUSE OF ACTION**
27 **Violation of the California Invasion of Privacy Act**
Cal. Penal Code § 632
28 **On Behalf of the Plaintiff and Classes**

1 135. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
2 same force and effect as if fully restated herein.

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

6 137. Section 632 defines “confidential communication” as “any communication carried on in
7 circumstances as may reasonably indicate that any party to the communication desires it to be confined to
8 the parties thereto[.]”

9 138. Plaintiff’s and Class Members’ communications with online services are confidential
10 communications for purposes of § 632 because Plaintiff and Class Members had an objectively reasonable
11 expectation of privacy in this data.

12 139. Plaintiff and Class Members expected their communications would not be shared with
13 Adobe, as there were no disclosures that Adobe would secretly eavesdrop upon or record their information
14 and communications.

15 140. Adobe’s tracking technology is an electronic amplifying or recording devices for purposes
16 of § 632.

17 141. By contemporaneously intercepting and recording Plaintiff’s and Class Members’
18 confidential and identifiable communications to online services through this technology, Adobe
19 eavesdropped and/or recorded confidential communications through an electronic amplifying or recording
20 device in violation of § 632 of CIPA.

21 142. At no time did Plaintiff or Class Members consent to Adobe’s conduct, nor could they
22 reasonably expect that their communications with online services would be overheard and recorded by
23 Adobe.

24 143. Adobe utilizes these private communications for their own benefit, including to serve
25 targeted advertisements and develop user profiles.

26 144. Plaintiff and Class Members have been harmed as a result of Adobe’s conduct. Their
27 private data has been intercepted, viewed, and used for targeted advertising and has not been destroyed.
28

1 Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored
2 and used, such that Plaintiff and Class Members have no adequate remedy at law.

3 145. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which
4 provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of damages sustained
5 by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable
6 relief.

7 **FIFTH CAUSE OF ACTION**
8 **Violation of the California Invasion of Privacy Act**
9 **Cal. Penal Code § 638.50 & 638.51**
10 **On Behalf of the Plaintiff and Classes**

11 146. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
12 same force and effect as if fully restated herein.

13 147. CIPA § 638.50(b) defines a “pen register” as a “device or process” that “records or decodes
14 dialing, routing, addressing, or signaling information” that is “transmitted by an instrument or facility
15 from which a wire or electronic communication is transmitted, but not the contents of a communication.”

16 148. Separately, CIPA § 638.50(c) defines a “[t]rap and trace device” as a “device or process
17 that captures the incoming electronic or other impulses that identify the originating number or other
18 dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or
19 electronic communication, but not the contents of a communication.”

20 149. CIPA § 638.51 prohibits a person from installing either a pen register or trap and trace
21 device without a court order.

22 150. Adobe is a person under CIPA § 638.51.

23 151. Adobe implemented and installed the ECID framework—which are pen registers and/or
24 trap and trace devices—on Plaintiff’s and Class Members’ devices and browsers.

25 152. These processes captured “routing, addressing, or signaling information” because they
26 intercept: (1) unique user and device identifiers; and (2) the Adobe Org ID (indicating the website to whom
27 the user is communicating).

28 153. Adobe was not authorized by any court order to use a pen register or trap and trace device
to record or capture Plaintiff’s and Class Members’ routing, addressing, or signaling information.

1 154. Plaintiff and Class Members did not consent to Adobe’s installation of a pen register or trap
2 and trace device on their devices and browsers.

3 155. Plaintiff and Class Members have been harmed as a result of Adobe’s conduct. Adobe did
4 not have authorization to use pen registers and/or trap and trace devices to surveille and identify Plaintiff
5 and Class Members or other routing, addressing, and signaling information revealing who the intended
6 recipients of their communications were.

7 156. Plaintiff and Class Members face an imminent threat of continued injury, as this data
8 continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

9 157. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which
10 provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of damages sustained
11 by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable
12 relief.

13 **SIXTH CAUSE OF ACTION**
14 **Violation of the Comprehensive Computer Data Access and Fraud Act**
15 **Cal. Penal Code § 502 (“CDAFA”)**
16 **On Behalf of the Plaintiff and Classes**

17 158. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
18 same force and effect as if fully restated herein.

19 159. The California Legislature enacted CDAFA to “expand the degree of protection afforded. .
20 . from tampering, interference, damage, and unauthorized access to ([including the extraction of data
21 from]) lawfully created computer data and computer systems,” finding and declaring that “the
22 proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of
23 unauthorized access to computers, computer systems, and computer data,” and that “protection of the
24 integrity of all types and forms of lawfully created computers, computer systems, and computer data is
25 vital to the protection of the privacy of individuals . . .” Cal. Penal Code § 502(a).

26 160. Plaintiff’s and Class Members’ devices on which Adobe’s tracking technology is installed,
27 including their computers, smart phones, and tablets, constitute “Computer system” within the meaning
28 of the CDAFA. *Id.* § 502(b)(5).

1 161. The data that Adobe accessed and collected from Plaintiff's and Class Members' devices
2 constitute "Data" within the meaning of the CDAFA. *Id.* § 502(b)(8).

3 162. Defendant Adobe violated § 502(c)(1) of the CDAFA by knowingly accessing without
4 permission Plaintiff's and Class Members' devices in order to wrongfully obtain and use their personal
5 data, in violation of users' reasonable expectations of privacy in their devices and data.

6 163. Defendant Adobe violated § 502(c)(2) of the CDAFA by knowingly and without
7 permission taking, copying, and making use of Plaintiff's and the Class Members' unique identifiers and
8 other personal data from their devices.

9 164. Defendant Adobe's tracking technology incorporated on Plaintiff's and the Class Members'
10 devices constitute "computer services" within the meaning of the CDAFA. Defendant Adobe violated §
11 502(c)(3) by knowingly and without permission using those computer services, and/or causing them to be
12 used. Defendant Adobe violated § 502(c)(7) by knowingly and without permission accessing those
13 devices, and/or causing them to be accessed.

14 165. Defendant Adobe violated §§ 502(c)(6) and (c)(13) of the CDAFA by knowingly, and
15 without permission from Plaintiff and the Class Members, providing and/or assisting in providing
16 advertisers and website owners the ability to access Plaintiff's and the Class Members' personal data via
17 its Tracking Technology.

18 166. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of
19 computer instructions that are designed to . . . record, or transmit information within a computer, computer
20 system, or computer network without the intent or permission of the owner of the information."
21 Defendants Adobe violated § 502(c)(8) by knowingly and without permission introducing a computer
22 contaminant via its tracking technology incorporated on Plaintiff's and the Class Members' devices, which
23 intercepted their personal data. As described *supra*, the tracking technology is deeply hidden; Plaintiff and
24 Class Members had no way to remove it or opt out of its functionality.

25 167. Plaintiff and Class Members suffered damage and loss as a result of Adobe's conduct.
26 Adobe's practices have deprived Plaintiff and the Class Members of control over their valuable property
27 (namely, their sensitive personal data), the ability to receive compensation for that data, and the ability to
28 withhold their data for sale.

1 168. Plaintiff and the Class Members seek compensatory damages in accordance with CDAFA
2 § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

3 169. Plaintiff and Class Members have also suffered irreparable and incalculable harm and
4 injuries from Adobe’s violations. The harm will continue unless Adobe is enjoined from further violations
5 of this section. Plaintiff and Class Members have no adequate remedy at law.

6 170. Plaintiff and the Class Members are entitled to punitive or exemplary damages pursuant to
7 Cal. Penal Code § 502(e)(4) because Adobe’s violations were willful and, upon information and belief,
8 Adobe is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiff and the
9 Class Members are also entitled to recover their reasonable attorneys’ fees under § 502(e)(2).

10 **SEVENTH CAUSE OF ACTION**
11 **Unjust Enrichment**
12 **On Behalf of the Plaintiff and Classes**

13 171. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
14 same force and effect as if fully restated herein.

15 172. Adobe receives benefits from Plaintiff and Class Members in the form of their unique
16 identifiers and other personal data and private online communications. Adobe acquired this information
17 without Plaintiff’s and Class Members’ authorization and without providing corresponding compensation.

18 173. Adobe acquired and used this private data for its own benefit, including tangible economic
19 benefits from companies that used Adobe for targeted advertising.

20 174. Had Plaintiff and Class Members known of Adobe’s misconduct, they would not have
21 agreed Adobe could acquire and use their private data.

22 175. Adobe unjustly retained these benefits at the expense of Plaintiff and Class Members.
23 Plaintiff and Class Members were harmed by this conduct and were not provided any commensurate
24 compensation.

25 176. The benefits Adobe received and derived from Plaintiff and Class Members’ private data
26 rightly belong to Plaintiff and Class Members. It is inequitable under unjust enrichment principles for
27 Adobe to retain the profits and other intangible benefits they derived through its wrongful conduct.

28 177. Adobe should be compelled to disgorge these profits and other inequitable proceeds in a
common fund for the benefit of Plaintiff and Class Members.

1 **EIGHTH CAUSE OF ACTION**
2 **Injunctive Relief**
3 **On Behalf of the Plaintiff and Classes**

4 178. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the
5 same force and effect as if fully restated herein.

6 179. Adobe’s conduct has and continues to cause harm to Plaintiff and Class Members’ privacy
7 and autonomy, as it continues to store unique persistent identifiers, as well as the private contents of their
8 communications, on its own systems. Adobe routinely uses this information for targeted advertising.

9 180. Accordingly, Plaintiff and Class Members seek injunctive relief, including an order
10 permanently restraining Adobe from continuing to use and store this information without consent and/or
11 a court order, and requiring Adobe to delete this information from its systems.

12 **PRAYER FOR RELIEF**

13 WHEREFORE, Plaintiff on behalf of himself and the putative Classes requests the Court enter
14 an Order:

- 15 a. Certifying the Classes and appointing Plaintiff as Class Representative;
- 16 b. Finding Adobe’s conduct unlawful;
- 17 c. Awarding injunctive and other equitable relief as is just and proper;
- 18 d. Awarding Plaintiff and the Classes statutory, actual, compensatory, punitive, nominal,
19 and other damages, as well as restitution and/or disgorgement of unjust and unlawful
20 profits;
- 21 e. Awarding pre-judgment and post-judgment interest;
- 22 f. Awarding reasonable attorneys’ fees, costs, and expenses; and
- 23 g. Granting any other relief as the Court sees just and proper.

24 **JURY DEMAND**

25 Plaintiff demands a trial by jury.

1 Dated: April 2, 2025

/s/ Willem F. Jonckheer

2 Robert C. Schubert S.B.N. 62684
3 Willem F. Jonckheer S.B.N. 178748
4 Amber L. Schubert S.B.N. 278696
5 **SCHUBERT JONCKHEER & KOLBE LLP**
6 2001 Union Street, Suite 200
7 San Francisco, CA 94123
8 Tel.: (415) 788-4220
9 Fax: (415) 788-0161
10 rschubert@sjk.law
11 wjonckheer@sjk.law
12 aschubert@sjk.law

13 Christian Levis (*pro hac vice* forthcoming)
14 Amanda Fiorilla (*pro hac vice* forthcoming)
15 Rachel Kesten (*pro hac vice* forthcoming)
16 Yuanchen Lu (*pro hac vice* forthcoming)
17 **LOWEY DANNENBERG, P.C.**
18 44 South Broadway, Suite 1100
19 White Plains, NY 10601
20 Tel.: (914) 997-0500
21 Fax: (914) 997-0035
22 clevis@lowey.com
23 afiorilla@lowey.com
24 rkesten@lowey.com
25 ylu@lowey.com

26 *Attorneys for Plaintiff and the Proposed Class*